DECLAWING THE DRAGON: WHY THE U.S. MUST COUNTER CHINESE CYBER-WARRIORS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Strategy and Space

by

JORGE MUÑIZ, JR., LCDR, USN
B.S., New York Institute of Technology, New York, 1998

Fort Leavenworth, Kansas
2009

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-06-2009	Master's Thesis	AUG 2008 - JUN 2009

4. TITLE AND SUBTITLE
Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
JORGE MUÑIZ, JR., LCDR, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
To what extent do the Chinese cyber-warriors--within the People's Liberation Army along with both state and non-state sponsored hackers/crackers--represent a viable threat to both the security and prosperity of our nation as a whole? In the past several years the Chinese have developed a myriad of both lethal and non-lethal cyber-weapons with the intention of denying or degrading an adversary's ability to use space-based intercommunication network platforms. The PRC and PLA have demonstrated a rapid expansion of their asymmetric operations, especially in the realm of Cyberspace. This paper will seek to ascertain the United States military's ability to defend and enforce our national interests, both in regards to our own domestic infrastructures as well as our partners abroad from Chinese-directed cyber-attacks.

15. SUBJECT TERMS
Chinese, China, People's Liberation Army, People's Republic of China, Cyberspace, Cyber-Warrior, Cyber-Weapons, Cyber-Attack, Electronic Warfare, Computer Network Operations, Information Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	85	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: LCDR Jorge Muñiz, Jr.

Thesis Title: Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors

Approved by:

_____, Thesis Committee Chair
COL Wayne A. Parks, M.S.

_____, Member
Bob A. King, M.B.A.

_____, Member
Plaudy M. Meadows III, Ph.D.

_____, Member
Timothy L, Thomas, M.A.

Accepted this 12th day of June 2009 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

DECLAWING THE DRAGON: WHY THE U.S. MUST COUNTER CHINESE CYBER-WARRIORS by LCDR Jorge Muñiz, Jr., USN, 85 pages.

To what extent do the Chinese cyber-warriors--within the People's Liberation Army along with both state and non-state sponsored hackers/crackers--represent a viable threat to both the security and prosperity of our nation as a whole? In the past several years the Chinese have developed a myriad of both lethal and non-lethal cyber-weapons with the intention of denying or degrading an adversary's ability to use space-based intercommunication network platforms. The PRC and PLA have demonstrated a rapid expansion of their asymmetric operations, especially in the realm of Cyberspace. This paper will seek to ascertain the United States military's ability to defend and enforce our national interests, both in regards to our own domestic infrastructures as well as our partners abroad from Chinese-directed cyber-attacks.

ACKNOWLEDGMENTS

First and foremost, I would like express my deepest appreciation to my family for their support throughout this past year. To my beautiful wife, Michelle, I thank you for your undying patience and resilience, for pushing me to keep focused and on track, for believing in me, even when I didn't believe in myself, and for putting up with all my senseless U.S.-China tirades over hundreds of lunches and dinners. Everything I've accomplished is because of you and your never-ending support, so dedicating this thesis to you is only a small token of my gratitude. To both our sons, Xavier and Ethan, thank you for your understanding and consideration during the long nights spent at the library with a mountain of lifeless books vice fishing or playing ball.

To my Thesis Committee, I wish to extend my sincere gratitude for each of your respective knowledge, expertise, and guidance throughout the year. For my Chair, Colonel Parks, thank you for keeping me on point, vice allowing my thesis to digress down a China-Taiwan rat hole, as it could have easily done. For Tim Thomas, thank you for your inspiring books that stirred me over 5-years ago to pursue further knowledge in this field of study. Finally, to Bob King, thank you for jumping in at the last minute to save my paper from utter destruction.

Last, but not least, to all my U.S./Singaporean Army brethren and our one token Air Force Major in Staff Group 14D, I've learned more this year than I ever thought I could. Each of you had more than a little part to do with this thesis, whether through loaning books, sharing your China-related knowledge and experiences with me, proofreading poorly written pages but encouraging me to not give up, or even arguing with me incessantly on the validity of the term "kinetic operations." Thank you!

TABLE OF CONTENTS

Page

ACRONYMS

CNA	Computer Network Attack
CNE	Computer Network Exploitation
CND	Computer Network Defense
CNO	Computer Network Operations
DDoS	Distributed Denial of Service
EA	Electronic Attack
ECM	Electronic Counter Measures
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
IO	Information Operations
INEW	Integrated Network Electronic Warfare
PLA	People’s Liberation Army
PRC	People’s Republic of China

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

The purpose of this paper is to determine to what extent the Chinese cyber-warriors--within the People's Liberation Army (PLA) along with both state and non-state sponsored hackers/crackers--represent a viable threat to both the security and prosperity of our nation as a whole. Additionally, this paper will seek to ascertain the United States military's ability to defend and enforce our national interests, both in regards to our own domestic infrastructures as well as our partners abroad, from Chinese-directed cyber-attacks; with special focus given to those systems critical to the Soldier on the battlefield. Finally, the paper will evaluate legal precedent, both internationally and domestic, in order to determine viable courses of action when confronted with an escalation of force in the Cyberspace.

There are many secondary questions which arise from the aforementioned thesis statements, such as how will China signal intent in situations involving their cyber-warfare capabilities? What thresholds should be established for an appropriate military response and what assets or tools do we have at our disposal to respond to these threats? If our current status or structure is insufficient, how does one propose reinforcing our U.S. Government capabilities to counter a Chinese threat?

Based on the subject matter in question, it is critical first and foremost that one clearly defines two major topics that are to be repeated throughout the thesis. First, on the term Cyberspace, Joint Publication 1-02 (as of October 2008) defines it as: A global domain within the information environment consisting of the: interdependent network of information technology infrastructures, including the Internet, telecommunications

networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08) This definition, however, is not a delimiter to the extent of what Cyberspace actually is. As such, and for the purposes of the remainder of this thesis, Cyberspace will encompass not only the actual military and civil electronics devices, but also the electromagnetic spectrum on which the information (be it either Command, Control, Communications, or Intelligence: C3I) travels to or from the end users. Additionally, the domain of Cyberspace must include the medium through which the C3I travels, be it wired, wireless, or space; and the associated defenses thereof. Therefore, space-based platforms along with their associated land-based controllers also reside in the Cyberspace domain. Finally, Cyberspace must include the physical platforms used to store, modify, and exchange data via networked systems and associated physical infrastructures.

A second critical concept to understand up front, and especially when evaluating the likelihood of a Chinese cyber-attack is that of the assassin's mace (shashoujian). The PLA endeavors for high-tech gear and knowledge; their focus is on six major areas, however the two directly related to this thesis are: military information technology and military space technology.[1] The PLA understand the role revolutions in military affairs have played in history, and they seek to identify those new combat methods that represent China's future "shock and awe;" devastating enough to deter any further U.S. military action in a crisis, but clearly decisive in its use of surprise. PLA Colonels Li Daguang and Jia Junming have both publically urged the development of an assassin's mace to "meet the requirements of defeating the United States in a war over Taiwan."[2]

Several major issues surfaced in 1999 when the PLA began incorporating offensive computer network operations (CNO) into military exercises, "primarily in first-

strike tactics against enemy networks."[3] The Chinese government, the People's Republic of China (PRC), has even issued a Chinese Defense Policy white paper that confirms what the U.S. Government has known for some time, that "[t]he PLA is carrying out a strategic project for training a large contingent of new-type and high-caliber military personnel… competent for operational tasks under conditions of informationization (sic)."[4] From the U.S. perspective, in 2007 General James Cartwright, Vice Chairman of the Joint Chiefs of Staff, has confirmed that "China is actively engaging in cyber-reconnaissance . . . of U.S. Government agencies."[5] Meanwhile, underground civilian organizations, from The Green Army to the likely state-sponsored Red Hacker Alliance (RHA), have participated in corporate and industrial espionage by "scanning for weaknesses in Pentagon information systems 'for fun.'"[6]

The problem with Chinese cyber-warriors is that the U.S. military relies heavily on unrestricted intercommunications networks, both military-controlled as well as non-military commercial systems, so too must we ensure their proper defense. However, in the past several years the Chinese have developed a myriad of both lethal and non-lethal cyber-weapons with the intention of denying or degrading an adversary's ability to use space-based intercommunication network platforms.[7] The PRC and PLA have demonstrated a rapid expansion of their asymmetric operations, especially in the realm of Cyberspace. What courses of action does the U.S. have prepared in the event of a Chinese cyber-war?

The Chinese Cyber-threat

The U.S. economy and national security are fully dependent upon information technology and the information infrastructure. Terrorists might attempt cyber attacks to

disrupt critical information networks, or attempt to cause physical damage to information systems that are integral to the operation of . . . commerce systems. Tools and methodologies for attacking information systems are becoming widely available, and the technical abilities and sophistication of terrorist groups bent on causing havoc or disruption is increasing.[8]

Having frequently been the target of several CNE attempts originating from PLA training centers to Beijing cyber-cafés, the U.S. has sustained damages ranging from Zero-Day Exploits,[9] to Distributed Denial of Service (DDoS) attacks, to Reverse Shell espionage. Unfortunately, the successful targets of such attacks have included the U.S. Department of Defense (DoD),[10] the U.S. Department of State,[11] and multiple private sector corporations.[12] As recently as 06 March 2009, in which Canadian researcher, Nart Villeneuve uncovered a network, dubbed GhostNet, of more than 1,200 infected computers worldwide which were unequivocally directed through servers located in China (one was controlled by a Chinese government server located in Hainan Island, a known PLAN submarine base).[13]

In addition to traditional computer targets such as the DoD's Non-Secure Internet Protocol Router Networks (NIPRNET), there are several non-traditional cyber-targets such as our U.S. satellite networks and military-grade electronic emissions that are paramount on the Chinese researcher's mission-set. Target sets such as these fall well outside the traditional hacker's capabilities. However, the PLA under their new directives, have been feverously developing anti-satellite capabilities of a lethal nature. From directed-energy (DE) high-powered microwave disruptors to free-electron and high energy lasers, [14] and from the lethal demonstrations of a DF-21 missile shoot-down of one

of their own aging weather satellites[15] to the mass development of $800 briefcase-sized transient electromagnetic devices (TED), [16] the face of warfare has changed.

As such, the U.S. military has made changes to expand beyond the operational concepts of strictly independent CNO, Electronic Warfare (EW), and Space Operations to instead be incorporated within the overarching and ethereal, but "physical," domain of Cyberspace. Not dissimilar to the domains of Land, Sea, and Air. There are now three mission areas in Cyberspace: counter-cyber operations, cross-domain operations, and support to civil authorities and the defense industry. [17]

This paper ultimately seeks to answer whether the U.S. military is capable of defending our national interests both domestically and abroad against a cyber-attack originating from Chinese cyber-warriors, either state sponsored or PLA-trained. Unfortunately, in this world of interdependent markets and economies on a truly global scale, those who would rely solely upon the benefits of the worldwide telecommunications network inevitably create vulnerabilities for themselves.[18] The same holds true for the Soldier or Marine relying on Blue Force Tracker for Command and Control (C2), GPS for navigation, INMARSAT for communication, or Predator feeds for situational awareness… or the Sailor relying on Naval Tactical Data Systems (NTDS) for over-the-horizon targeting, Bridge to Bridge (B2B) for maritime navigation, Voyage Management System (VMS) for transit routing, or the Global Command and Control System (GCCS) for situational awareness and command and control (C2). While each method rides over different mediums and on different frequencies, each taking up different quantities of bandwidth, they all reside in the aforementioned domain of Cyberspace.

The Nationalist Cyber-Terrorist

The Chinese hacker origins date back to 1994 when the Internet was first became available to the PRC. Back then, access was severely limited to those with enough money to afford, and patience to endure, the 9,600 bit/sec modems. This access was further limited to Bulletin Board Systems, the precursor to the World Wide Web.[19] Chinese restrictions on Internet access were lifted two years later; bringing the Internet into the homes of millions. It was the following year, 1997, that the Green Army[20] was founded. Self-proclaimed as one of China's earliest hacker organizations with a membership of over 3000 people from Shanghai, Beijing, and Shijaizhuang, this "enduring symbol of the Chinese hacker movement"[21] disbanded in 2000 due to financial hardship. However, this was not before a loose quasi-coalition of confederated hackers joined forces in response to the 1998 riots in Jakarta, Indonesia.

Blaming the PRC for their out of control inflation, the citizens of Indonesia directed a massacre against their own Chinese nationals. The Chinese governments chose to filter the incident from public view, but not before the atrocities were broadcast over the Internet. Essentially, a virtual Chinese Hacker's Emergency Conference[22] was held resulting in a military-type cyber-envelopment using e-mail Logic Bombs. Postings on many major Indonesian websites included such:

Your site has been hacked by a group of hackers from China. Indonesian thugs, there can be retribution for your atrocities, stop slaughtering the Chinese people.[23]

Seeing this as a viable, non-lethal alternative to protracted conflicts, the PRC began emphasizing a concept of Comprehensive National Power[24] whereby both the military and the civilian roles become integrated on behalf of the nation. State-

sponsored, but civilian, organizations quickly and gladly assumed the role of protector of national interests. Chinese hacker groups such as the Honker Union of China, the Red Hacker Alliance, and the Chinese Red Guest Network Security Technology Alliance would seek out targets of opportunity to attack. [25] It was therefore only a matter of time before the U.S. Armed Forces became the targets of their coordinated wrath.

In 1999, after U.S. planes bombed Beijing's embassy in Belgrade, Chinese hackers quickly commenced cyber-battles with their respective U.S. counterparts. [26] In 2001, following the mid-air collision of a U.S. EP-3 and a Chinese AN-124 on April 1st, the ensuing political conflict between the two powers prompted Chinese nationalists to rise up once again. Hackers soon after organized a massive week-long campaign of cyber-attacks against over 1200 U.S. sites to include the White House, U.S. Air Force, Department of Energy, Department of Labor, and Department of Health and Human Services. [27]

Assumptions

There are several assumptions that must be presented up front if we are to presume this thesis to be valid. First, the PRC has actively exploited the Microsoft Office source codes with the malicious intent of using them against the United States Government. Additionally the PRC sees cyber-warfare a first-strike option and is training and equipping the PLA in the conduct of such. With regards to Chinese "hacktivism," despite the fact that DoD and security officials remain divided over (1) whether the known cyber-attacks are coordinated or sponsored by the Chinese government, (2) whether they are the work of individual and independent hackers, or (3) whether the cyber-attacks are being initiated by some third-party organization that is

using network servers in China to disguise the true origins of the attacks, this thesis must assume at a minimum that the PRC is either fully aware of their existence or actually provides the mechanisms for their actions through either financial, informational, or via protection of those non-military individuals with the specific intent that they continue to conduct both Computer Network Exploitations (CNEs) and CNAs against the U.S. Government.

Limitations

In limiting the depth of this thesis, the focus will primarily be on those cyber-activities between the U.S. and China when not involved in an official state of war or involved in undeclared conflict. That implies that the thesis will not cover those PRC activities intended to assist non-state actors through funding, intelligence, or protection by the PRC and whose cyber-goals are operations intended to probe or attack the U.S. In addition, it will not evaluate the use of force by the U.S. military against recreational hackers, terrorists, or organized cyber-criminals as those comprise a law enforcement issue which must be addressed through bilateral extradition vice military action.

Another limitation is that all discussions will be restricted to actions initiated from within the borders of China. Therefore, U.S.-originated domestic cyber-activities will not be included; this consists of those domestic actions that are of direct assistance in a coordinated Chinese cyber-attack. Domestic CNE, again even in direct support of a coordinated Chinese cyber-attack, will also not be discussed because it is a domestic law enforcement issue. Neither will any other aspect of Information Operations (IO, Military Deception, Psychological Operation, or Operational Security) be discussed with the exception of how cyber-activities can be used to support IO.

Background: Taiwan and the Prelude to Cyber-War

It would be a stretch to imply that current cyber-tensions between the U.S. and China are simply due to the continued existence of the island-nation of Taiwan. However, it would also be a mistake to completely dismiss the events which have shaped the environment in the Far East since World War II. That said, in 1949 the former leader of China, Chiang Kai-shek, fled mainland China and relocated the Republic of China's (ROC) seat of government to the island of Taiwan, formerly known as Formosa. Kai-shek continued to claim sovereignty over all of mainland China from his island-hideout in Taipei, Taiwan.

Mainland China, however, had other plans for the island following the Chinese Civil War in 1949, in which the victorious Communist Party of China gained complete control under Mao Zedong. Mao moved to establish the People's Republic of China (PRC) and claim sole representation of China to include Taiwan, to which Zedung would assert, was illegitimately led.[28] Taiwan remained under martial law from 1948 until 1987, when Chiang Kai-shek's eventual successor, Lee Teng-hui, began the gradual democratization and liberalization of the ROC's governmental system. However, it was then that the controversial issues surrounding the political status of the Taiwanese government resurfaced. Beginning with the banking system, Teng-hui authorized the printing of banknotes from the Central Bank rather than the Provincial Bank of Taiwan. Soon after, President Teng-hui forced the disbanding of the Taiwan Provincial Government as well as demanding the resignations of the Legislative Yuan and National Assembly . . . both of whom were established in 1947 to represent mainland Chinese

constituencies. Finally, Teng-hui lifted all restrictions on the use of the Taiwanese language in both broadcasting and schools.

This entire discussion of Taiwan, to include their assertions of sovereignty from mainland China, ultimately resulted in one of the most significant military standoffs involving the U.S. and China. The root cause stemmed from a simple visit to Cornell University by the President of Taiwan, Lee Teng-hui. The People's Republic of China (PRC) took this visit as a serious affront to their communist-orthodox definition of what Taiwan's place in the world was. The PRC had expected that then-President Bill Clinton would block Lee's visit for the betterment of U.S.-China relations, but he did not. China very soon thereafter became engaged in a series of aggressive military demonstrations involving the firing of 6 ballistic missiles impacting just 80 miles off the Taiwanese coast. President Clinton understood that he could no longer assume peace in the Taiwan Straits and that the seemingly innocent visit had triggered deep emotional reactions between the two sides, with the U.S. in the middle.[29]

Believing power-projection to be the appropriate response to PRC aggression, U.S. leaders ordered two U.S. carrier strike groups to maneuver between the narrow waters separating Taiwan from mainland China--the Taiwan Straits. Lee sought to reassure the PRC that he did not intend to declare independence; Clinton sought to convince the PRC that we wanted to retain good relations with China, however, he was ready to defend Taiwan if needed.

---

[1]Frederic Vellucci, Collins Ferguson, Daniel Hartnett, and Kenneth Allen, *The Science of PLA Training: Analysis and Overview of PLA Training Theory* (Center for Naval Analysis, China Studies, February 2009), 132-133.

[2]Michael P. Pillsbury, "An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines," Report to the U.S.-China Economic and Security Review Commission, 19 January 2007, 22

[3]Sharon Gaudin, "China to Use Computer Viruses as Cyberwarfare Strike First," *Newspaper*, 29 May 2007,

[4]*China's National Defense in 2006*, Chapter 2, http://www.china.org.cn/english/features/book/194421.htm (accessed 22 May 2009)

[5]2007 Report to Congress of the US-China Economic and Security Review Commission (USCC), November 2007, http://www.uscc.gov/annual_report/2007/report_to_congress.pdf (accessed 22 May 2009).

[6]Melinda Liu, "High-Tech Hunger," *Newsweek 16* January 2006, http://www.newsweek.com/id/47443/page/3 (accessed 22 May 2009).

[7]Annual Report to Congress: Military Power of the People's Republic of China 2008, Office of the Secretary of Defense, 21.

[8]The National Strategy for Maritime Security, 20 September 2005, http://www.whitehouse.gov/homeland/maritime-security.html (accessed 18 October 2008).

[9]Ted Bridis: USA Today, *State Department Got Mai – and Hackers* http://www.usatoday.com/tech/products/2007-04-18-2250474372_x.*htm* (accessed 22 May 2009).

[10]Dawn S. Onley, and Patience Wait, Government Computer News, *Red Strom Rising* http://www.gcn.com/print/25_25/41716-1.html?page=2 (accessed 18 October 2008).

[11]Bridis.

[12]Bill Brenner Search Security, *How the China Syndrome Doomed 3M Merger Deal*, 21 February 2008, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1301833,00.html (accessed 18 October 2008); 2007 Report to Congress, USCC, 96.

[13]Omar El Akkad: *Canadian Researcher in Toronto Uncovers Worldwide 'Cyber-Spy Network'* (The Globe and Mail, Toronto) 30 March 2009.

[14]2007 Report to Congress, USCC, 97.

[15]David Kestenbaum: *National Public Radio, Chinese Missile Destroys satellite in 500-mile Orbit* http://www.npr.org/templates/story/story.php?storyId=6923805 (accessed 22 May 2009).

[16]David Schriner, Before the Joint Economic Committee, United States Congress, on 25 February, 1998, http://www.freedomdomain.com/weathercontrol/jointhearing.html (accessed 22 May 2009).

[17]David T. Fahrenkrug, Lt Col, USAF, http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html (accessed 18 October 2008).

[18]Walter Gary Sharp, Sr. *Cyberspace and the Use of Force* (Aegis Research Corporation, 1999), 17.

[19]Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers*, 8-51.

[20]Ibid., 12.

[21]Ibid., 13.

[22]Ibid., 16.

[23]Indonesian website, www.kobudi.co.id on 24 October 2005 and posted on www.juntuan.cn/user1/2344/archives/2005/9612.shtml (accessed on 22 October 2008).

[24]Henderson. 103.

[25]"Cyber Attacks During the War on Terrorism: A Predictive Analysis" (Institute for Security Technology Studies at Dartmouth College, September 22, 2001), 8.

[26]Simon Elegant: *Enemies at the Firewall* http://www.time.com/time/magazine/article/0,9171,1692063,00.html (accessed 25 January 2009).

[27]US Spyplane Crashing Chinese Jet: Pro-China Hackers Invade US Government Website, http://www.china.org.cn/english/12150.htm (accessed 22 May 2009).

[28]*PRC Taiwan Affairs Office and the Information Office of the State Council* (2005).

[29]Richard C. Bush and Michael E. O'Hanlon, "A War Like No Other: The Truth About China's Challenge to America" (John Wiley & Sons, Inc. 2007), 1-5.

CHAPTER 2

LITERATURE REVIEW

The purpose of this paper is to determine to what extent the Chinese cyber-warriors represent a viable threat to both the security and prosperity of our nation as a whole. To shape this effort, Chapter 2 will introduce in detail a myriad of literature covering the three main cyber-threats originating from China (again, recalling that this thesis will not evaluate recreational hacktivists) ; these are the People's Republic of China, the PLA, and the state-sponsored Chinese nationalist (or Honker). Each will be covered in the sub-chapter of China on China.

The paper, more importantly, seeks to ascertain our ability to defend and enforce our national interests, both in regards to our own domestic infrastructures, as well as our partners abroad, from Chinese-directed cyber-attacks. To that end, this chapter will also cover the current legal implications both domestically and internationally with regards to the U.S. military and their use of force in Cyberspace. Additionally, the literature review will also incorporate those specific national interests that would require defending with respect to Cyberspace both domestically and abroad.

Chapter 2 is broken down in three distinct sub-chapters representing either their author's predominant point of view or their primary literature's focus and they are labeled: China on China, United States' Perception of China, and finally, United States on the United States. This holistic approach is intended to not only satisfy the requirement of a literature review, but also to shape the reader's understanding as to the depth and give the reader insight into the complex nature that is Cyberspace.

China on China

This sub-chapter will review the literature originating from within the borders of China and specifically those books or articles covering such topics as the leadership within the PRC and the guiding Generals within the PLA who execute their direction. First of all, it is important to note that the PLA publishing system consists of 28 publishing houses; 16 newspapers (such as *PLA Daily*); and hundreds of periodicals[1] (such as *China Militia* and *China Air Force*). Their breadth represents an essential component of the PLA's ability to function as an institution. Unfortunately, for the purposes of research, it is important to note that the PLA publishing system has also been used to exercise political control and disseminate propaganda to both the Chinese population as well as to the rest of the world, to maintain organizational cohesion amongst the PLA services, to reform and modernize their officer corps through professional development, and to serve as civil-military proxy between the civilian population and the PLA that are tasked to defend them[2]. The PLA leadership views propaganda as a capability through which they can externalize their "soft power" while countering negative criticism as this *PLA Daily (Jiefangjun Bao)* article states that propaganda is "an important channel through which the PLA can improve its soft power and display the good image of the Chinese soldiers."[3]

Figure 1. The seven Chinese Military Regions
Source: Wikipedia, http://commons.wikimedia.org/wiki/File:China%E2%80%99s_Military_Regions.png (accessed on 18 March 2009).

All books and articles--even those written by military subject matter experts--are still vetted through the General Political Department (the GPD, who incidentally also oversees the Propaganda Department) who supervises, or censors, each publication before going into the PLA publishing system. Therefore, while the quantity of usable information specific to the thesis topic seems to be limited, it is actually the credibility of the information found in PLA books and publications that is of greatest concern.

PLA on Unrestricted Warfare

Rarely, a whole book manages to either circumvent the GPD vetting process, or is intentionally released for psychological purposes in an effort to satisfy United Nations (U.N.) Resolution 35/142B (Military Transparency). One such book, *Unrestricted Warfare* (超限战, literally "warfare beyond bounds") was initially published by the PLA Literature and Arts Publishing House in Beijing (Figure 1), and therefore suggests that it was endorsed at least by some elements of the PLA leadership. It is a book on military strategy that was authored, in part, as a response to the PLA's fascination with our successes in the first Gulf War. Written in 1999 by two colonels in from the PLAAF, Qiao Liang (乔良) and Wang Xiangsui (王湘穗), it reveals how China believes it can overcome our military's technological advantages and defeat the U.S. through a myriad of "total warfares;" the two of which most directly apply to this thesis: technology warfare and network warfare. However, Qiao and Wang are not so rudimentary as to stop there. They go on to overtly imply, for example, that the attacking side of two developed nations might employ strictly military force-on-force techniques that incorporate "satellite reconnaissance, electronic countermeasures, large-scale air attack plus precision attacks, ground outflanking, amphibious landings, [and] air drops behind enemy lines."[4] Contrary to the force-on-force, they suggest a better alternative in the form of a "combination method" that includes not only military techniques, but also trans-military and non-military capabilities. They therefore suggest that:

> If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity

> network, traffic network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis.[5]

This example ends with the attacking military force bearing down on the vanquished foe until a "dishonorable peace treaty" is signed. This is the crux of *Unrestricted Warfare* and the Chinese cyber-warrior represents the first in a line of viable "combinations" that can be used against the U.S. and her allies.

Finally, with respect to "Unrestricted Warfare," Qiao and Wang proceed to describe "kinder weapons" to which they suggests a tank's combat capabilities can be hard destroyed with either a missile or cannon, however, a kinder option would be to destroy its optical equipment with a directed energy weapon. Under kinder weapons, he suggests that there are two flavors: "hard destruction" as in an electro-magnetic pulse (EMP), and reversible "soft-strikes" as in computer logic bombs, network viruses, or DDoS attack. "Both [he claimed] are focused on paralyzing and undermining, not personnel casualties."[6]

PLA on Information Operations

Essentially, the "Research on Information Warfare Issues in Our Military" (Wojun Xinxizhan Wenti Yanjiu) is a compilation of some of China's most prominent Information Operations theories and practices as they apply to the PLA. Its editor, Peng Chencang, pulled from several dozen experts, however, none as prominent or outspoken as then-Major General Dai Qingmin. Dai elaborated on the exploitation of the Battlefield Information Environment (BIE) to gain combat advantage. He goes on to assert that there are three elements that compose the BIE; they are the fields of electromagnetism,

computers and their networks, and human society (which will not be covered in this thesis).

Dai claimed that it is the electromagnetic field, which he also coined as the "main field," in which BIE exists. He also asserted that in future combat, China will face an electromagnetic signal space with denser and more complex signals. For example, he lists not only the electromagnetic waves, but also light and sound waves as well. On the topic of computers and their associated networks, Dai believed that on future battlefields there will become a huge reliance on both the information processing and dissemination via Cyberspace; resulting in new types of combat such as "hacker warfare, network warfare, and computer virus warfare."[7] This all seems very rudimentary, that is until Dai explains how the BIE has its own unique characteristics and capabilities, thereafter mimicking the sentiments of Qiao and Wang's *Unrestricted Warfare* once again.

In *Unrestricted Warfare* the reader is introduced to the concept of "combination methods" in which an enemy nation could be met with not only cyber-warfare, but also diplomatic, financial, trade, drug, terrorist, ideological, and even ecological warfare. Dai, in his submission echoes these sentiments by overtly bringing in the factor of "domestic combat information systems" (or nationalist Chinese "Hacktivists") into the fold. Dai claims that within the information era the "fusing and sharing of military and commercial information facilities and technologies [so that] the boundaries between military, non-military, global and BIE will gradually become ambiguous."[8] Dai describes pieces of China's possible Course of Action (COA) utilizing what can only be construed again as Chinese nationalists by conducting an "invasion, attack, and damage of enemy classified

information networks [using either] opposing military organizations (PLA) or from an unknown hacker with no association to any government."[9]

Dai, without directly saying either the U.S. or Taiwan, successfully calls out both nations:

> …whether for counter-invasion warfare or unification or the motherland, we will stand our ground in homeland combat. Contrary to the enemy, which will undergo a long mobilization away from home, we have the factor of convenience in utilizing the foundational information facilities . . . all can be converted for military use in wartime.[10]

Dai expounds on this rhetoric just one year later when he called upon uniting civilian and the PLA under a single common telecom system to meet both peacetime and wartime needs. In Dai's "Innovating and Developing Views on Information Operations" he defines the "target" as the military information and information systems, and the "principal form[s]" encompassing both EW and CNO. He also emphasized that future operations must be integrated, meaning both military and civilian fighting forces. Finally, Dai lays out ten cyber-stratagems as follows: plant information mines, conduct information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information, organizing information defense, and establishing network spy stations.[11]

PLA in Chinese Periodicals

The *PLA Daily (Jiefangjun Bao)* and *China National Defense News* are the only two PLA newspapers designated and written specifically for public consumption (gongkai; 公开). Public distribution of these newspapers began in 1987, with the goal of giving the general public the opportunity to read about PLA affairs in a state-sponsored

publication. Since then, this goal has been furthered by the introduction of Internet editions, such as the *PLA Daily* online edition, which is also available to the Chinese public.[12] In a March 2007 *PLA Daily* Online article, the former-director of the Chinese PLA Communications Department and current director of the PLA's Advisory Committee for Informationalization, Major General Dai Qingmin (a known advocate of the pre-emptive cyber-attack to gain the initiative and seize information superiority[13]) was interviewed on both network and national security. During the interview he revealed the development of computer operating systems that are completely self-dominated and free of intellectual property rights (an open sourced Linux-style operating system, for example) as well as the development of an internal (military) professional training system[14] relating to the topic of "informationalization" (sic).

Over the past several years, *PLA Daily* has, along with several other well-read Chinese periodicals, documented the growth and development of their armed forces. For example, since post 9/11, the *Hong Kong Journal* began an in depth analysis of the Taiwanese "Hankuang 18" exercises. This 2002 journal emphasized Taiwan's participation in a computer network warfare training exercise codenamed "Lusheng II." The PLA General Staff Department quickly directed relevant combat units of the PLA to study and analyze the "Lusheng II" warfare tactics, and to come up with countermeasures as quickly as possible. However, the same article backs current Chinese research and development by reminding their readers of three main points: first, the China's maturing satellite technology with surveillance and future positioning capabilities; second, the establishment of specialized IW units tasked with both developing computer viruses to sabotage enemy computer systems as well as guarding the PLA's computer systems; and

finally, the development of institutions of higher learning with regards to IW, such as the PLA Information Engineering University, which had at the time "developed unique characteristics in . . . information security . . . telecommunications engineering . . . and space information and surveying technology"[15]

Chinese periodicals have also indicated a vested interest by the PLA in counter-reconnaissance and active surveillance jamming techniques. The first of these deception means, counter-reconnaissance, involves passively applying advanced camouflage techniques coupled with natural environmental conditions to defeat U.S. reconnaissance systems. While this is not a traditional application of PLA cyber-warriors, their efforts signal intent to develop passive asymmetric counter-Cyberspace means. For example, the Jinan Military Region (MR, Figure 1) held their region's Winter Field Training exercise in 2007 where all three armies (20th, 26th, and 54th) held counter-reconnaissance drills against "high-tech reconnaissance means."[16] The *PLA Daily* covered the same period, focusing on the 54th Group Army. The 54th carried out innovative, although questionably useful, countermeasures such as road-side dispersals, creating smoke screens, hiding in ravines, and even intermixing with civilian tragic on highways.[17]

During times of war or national emergency, War Zone Headquarters (WZHQ) will be established based primarily on the Military Regions (Figure 1). The WZHQ will have command of all forces in all branches of service in their respective regions. Similar to U.S. military operations, the PLA divides military operations into phases according to terrain, task, or time (reminiscent of Milan Vego's: space, force, time). Dennis J. Blasko explains in his 2006 The Chinese Army Today that WZHQ, beyond traditional military

units, may employ local forces (People's Armed Police), as well as militia augmented by civilian forces[18] (which does not preclude the nationalist cyber-warriors). *PLA Daily*, in 2007, covered the PLAAF's enlistment of their militia in the Tangshan Military Subdistrict (Beijing MR, Figure 1) to assist in camouflaging air defense positions. In this case, the militia also used dubious means to obscure their adversary's bomb damage assessment, which included fire, lights, smoke, and electronics to "hide or transform the shape of important infrastructures, such as oil depots, power plants, and bridges."[19]

The second deception means, active surveillance jamming techniques, certainly fall within the domain of Cyberspace. In an interview with Bingqi Zhishi an "expert" suggested that it was possible to electronically jam the telemetry control signal between ground control and surveillance satellites. Taiwan's *Taipei Tim*es reported in 2006 that Chinese have already developed a form of laser dazzling and have used that technique on U.S. military satellites.[20]

On issues of electronic warfare (EW), however, the Chinese research and development has clearly recognized the increasingly greater role that both EW and electronic counter measures (ECM) play in a modern warfare. In the Chengdu MR (Figure 1), experiments are still ongoing to test and evaluate the jamming effectiveness from the jamming side. In an article published in the *Dianzi Xinxi Juikang Jishu*, several renowned scientists and scholars challenged the traditional jamming parameters of measuring signal-to-noise interference ratio at the receiver, max transmission range at the transmitter site, detection zone (specifically for radar systems), the suppression coefficient, the discover probability, and the deceit probability.[21] Instead, they propose that this method is only effective in a field test situation and is essentially worthless in a

war as "the jamming side cannot possibly obtain these evaluation data on the enemy… directly."[22] The authors, Li Chao and Zhou Jinquan, are research scientists for the Missile Institute of Air Force Engineering University and the Military Academy of the PLA, respectively. So their insight and analysis most-closely resembles what one should expect to encounter when facing and informationalized PLA.

The aforementioned periodical also published an article on the "Multi-Signal Jamming Technology in [a] Complex Environment" written by Li Dongxin, a researcher from the National Keu Lab of Information Integrated Control in the Chengdu MR (Figure 1). In it, Dongxin reviews the two main radar jamming technologies used for PLA ECM: multi-pulse velocity-range decoys and multi-pulsed false target jamming. Either technique is intended to target a pulsed-Doppler radar system's (the non-phased array systems still used by our military forces) capability to not only detect target location (bearing, range, and altitude) but also a target's radial velocity (range-rate). Specifically, Dongxin's conclusion is that in an increasingly complex multi-signal environment, ECM equipment has no choice but to make fundamental improvements.[23]

Finally, on the topic of direct sequence spread spectrum (DSSS) signals, the same periodical published an article on "DSSS Signal Parameter Estimation" written by Chen Ximing and Huang Shuoyi. In it they admit that both detection and parameter estimations have become a difficult problem, especially as they relate to jamming. Unfortunately, this form of digital communication serves an essential role in both U.S. military (GPS and Galileo) and civilian (CDMA, LRCP, 802.11b, etc) purposes. DSSS provides secured communications, multi-address communications, and satellite navigation and location. Ximing and Shouyi ultimately assert that one of the key steps in

conducting non-cooperative communications (or simply electronic surveillance, ES) is to "obtain signal modulation parameters, code period, chip rate, and carrier wave frequency."[24]

On the topic of the most recent scandal, the blatant and highly publicized Chinese cyber-spying via zombie U.S. and Chinese servers, also known as GhostNet, China quickly countered through a myriad of publications. First, in the most widely read China Daily, military analyst and Beijing-based strategist Song Xiaojun claimed that "this [was] purely another political issue that the West is trying to exaggerate [and] as China grows, some in the West are trying every opportunity to manufacture fears over China's threat."[25] Second, in an interview with Professor Zhu Feng, from the School of International Studies in Peking noted that "cyber security has been a global issue . . . those who see China as an emerging threat again [have] picked the new subject as a weapon."[26] Finally, in Beijing's *Global Times (Huanqiu Shibao)* information security expert, Qiu Feng, pointed out that ". . . creating such a huge network and (sic) organizing personnel and coordinating attacks in different countries is not an easy matter. . . . This story is full of loopholes. There is insufficient evidence to say that China has such a huge overseas spy network."[27]

United States' Perception of China

> [The] goal of a space shock and awe strike is [to] deter the enemy, not to provoke the enemy into combat. For this reason, the objectives selected for strike must be few and precise . . . [for example] on important information sources, command and control centers, communications hubs, and other objectives. This will shake the structure of the opponent's operational system of organization and will create huge psychological impact on the opponent's policymakers.[28]
>
> -- Colonel Zelu,, PLA, National Defense University

The PRC's interpretation with respect to what constitutes either an attack or the legitimate use of force is vague at best. In the 2008 Annual Report to Congress on the Military Power of the People's Republic of China (ARC 2008), we are reminded of China's history (Korean War, 1950-1953; Indian conflict, 1962; Soviet conflict, 1969; Vietnam, 1973) in which they charge their PLA with either the preemptive or coercive use of force in an effort to advance their own core interests. The ARC 2008 overtly implied that Chinese precedent demonstrates their territorial claims on Taiwan, quoting Chinese Military theory "if any country or organization violates the other country's sovereignty and territorial integrity, the other side will have the right to 'fire the first shot' on the plane of tactics."[29]

The ARC 2008 goes on to include vague references to China's "Assassin's Mace" (shashoujian) Programs in which part of the PLA's asymmetric warfighting strategy is to use programs designed to give technologically inferior militaries advantages over technologically superior adversaries. Since 1999, the ARC 2008 notes, the term has appeared more frequently in PLA journals. Although not clearly specified in the ARC 2008, China's "Assassin's Mace" would likely be a mixture of old and new technologies applied in unique ways, "particularly in the context of fighting the United States in a Taiwan conflict."[30]

U.S. on the Modernization of the PLA with respect to CNO

On CNO, the 2008's *Report to Congress from the U.S.-China Economic and Security Review Commission (USCC 2008)* acknowledges the critical vulnerability of the U.S. Government and economy due to our heavy dependence on the Internet. As such,

the USCC 2008 presumes that China will likely seek to take advantage of this U.S. reliance due to the following assessments:

1) The costs of Cyberspace operations are low in comparison with traditional espionage or military activities.
2) Determining the origin of cyber-operations and attributing them to the Chinese government or any other operator is difficult; hindering our response.
3) Cyber-attacks can be used to confuse us, the enemy.
4) There is an underdeveloped legal framework to guide responses

As such, China is very likely to continue pursuing CNO capabilities that may provide them with an asymmetric advantage against the U.S.

As noted by Wang and Qiao in *Unrestricted Warfare*, China's perception of U.S. success in the first Gulf War led to a growing number of CNO advocates amongst PLA officials. Mark A. Stokes from the Strategic Studies Institute, and former U.S. military attaché in Beijing, wrote back in 1999 on the Chinese enthusiasm and the concurrence that called for the development of weapons systems that can "throw the financial system and army command systems of the hegemonists (sic) into chaos." Stokes goes on to note that technological weapons of this nature provide an asymmetric advantage for an underdeveloped country to use against a nation which is "extremely fragile and vulnerable when it fulfills the process of networking and then relies entirely on electronic computers."[31] PLA strategists, according to Stokes, have thus increased their emphasis on computer warfare and have expanded to include the feasibility of introducing computer viruses (bingdu) via wireless means. Stokes' assessment, written at the same time that *Unrestricted Warfare* was published mimics the sentiments of Wang and Qiao on combined warfare with specificity towards Financial Warfare + Network Warfare.

China's most recent cyber-snooping escapade painted the PRC into the proverbial corner as the Canadian researcher, Nart Villeneuve, learned about the GhostNet infiltration network through the use of honey-pots. Toronto's *The Globe and Mail* revealed how Villeneuve's "honey-pot" computers were taken over. Mysterious entities sought to reveal the honey-pots' processor speed, memory specifications, geographic information as to its location, 'My Documents' files, and finally given an instruction to download a copy of the GhostNet remote-access tool. Villeneuve's evidence showed that the majority of the "control servers were located in China . . . [and] the interface to control the infected hosts on these servers in China was in Chinese," and finally, the "remote Trojan favoured (sic) by the attackers is a Trojan coded by Chinese hackers."[32] However, most disturbing of all was neither Chinese servers nor the Chinese-coded Trojans; rather, the high value targets which include none other than Deloitte & Touche, employer of over 165,000 professional in 140 countries delivering audit, tax, consulting, and financial advisory services through its member firms.[33] Recalling Qiao and Wang's suggestion presented in *Unrestricted Warfare* of using a combined warfare, such as network warfare with financial warfare.

U.S. on the Modernization of the PLA with Respect to EW

Chinese research and development clearly recognizes the greater role that electronic warfare plays on the informationalization of their PLA. U.S. literature also recognizes that Chinese leaders have prompted to accelerate the modernization of their armed forces. For example, the Center for Strategic and International Studies published *Chinese Military Modernization* in 2007, which emphasized the PLA force development and strategic capabilities. As such, there is significant concentration in the development

of the PLA's technological base with emphasis on C4ISR.[34] This statement is supported in the U.S. DoD Annual Estimates of Information Warfare Capabilities and Commitment of the PRC 2002-2009 where the author, Dr. Kabay, highlights the PLA's objective to seize electromagnetic dominance. He described the combination of electronic warfare, CNO, and lethal strikes as Integrated Network Electronic Warfare (INEW).

U.S. on the Modernization of the PLA with Respect to ASAT and Space

The *ARC 2008* noted that China has developed significant ASAT capabilities that go far beyond those demonstrated by the direct-ascent shoot down of January 2007. They include co-orbital kinetic weapons, directed energy weapons (both of which are still under development) and micro-satellites. China is also developing electronic attack and CNO techniques targetting an adversary's space assets as well as its ground support networks. Finally, the ARC 2008 believes that the PLA consider ''battlefield situational awareness'' so critical to modern combat operations that the development of an offensive "Assassin's Mace" weapon, specifically with space attack capability is required.

In an effort to counter our national interests in space, the PLA has developed multi-dimensional space programs focused on limiting or preventing the use of satellite-based assets by their potential adversaries during times of conflict.[35] Designed to exploit a number of susceptible space assets, their research and development fall into two basic categories of lethal-kill methods: either directed-energy or direct-ascent. Non-lethal methods, however, targets one of two specific subcomponents of an adversary's space collection capabilities: imagery collection, or signals intelligence (SIGINT) collection. The Chinese have even expanding their CNO initiatives to include activities that threaten the DoD's space control and supporting computer networks, thus posing a significant risk

to critical U.S. warfighting systems. Thankfully, U.S. military satellite communications space assets are physically hardened or software protected in an effort to counter such vulnerabilities… unfortunately, however, few of the U.S. military's commercially-leased systems share this level of hardening.[36] Thus, this brings China's space capabilities and militarized intentions to a level of U.S. national interest, and the aforementioned threat to our security and prosperity of our nation as a whole.

Although the PRC has never publically acknowledged a dedicated anti-satellite (ASAT) program, the PLA has been intently interested in building the capacity to deny, degrade, deceive, disrupt, delay, corrupt and even destroy their adversaries' use of space based satellite platforms and their associated systems. The research and development to achieve this has been ongoing since the 1960s; likely assisted by Mao Tse Tung's mid-1950s ABMD rhetoric. Under their anti-ballistic missile defense (ABMD) 640 Program of 1963, the PRC made their first attempts to build a system consisting of a lethal "kill" vehicle, high powered lasers, and a space indications and warnings (I&W) network[37]. Although the ABMD 640 Program was abandoned in the 1980's, the technology developed set the stage for transition into China's High Technology Development 863 Program under Deng Xiaoping.

Dr. Michael Pillsbury, a Senior Fellow for the Atlantic Council of the U.S. and Associate Fellow for the National Strategic Studies Asian Affairs, authored An *Assessment of China's Anti-Satellite and Space Warfare Program* in 2007. Although his assessment was not submitted to the U.S.-China Economic and Security Review Commission until a week after the Chinese ASAT incident of 2007, the depth and breadth to which Pillsbury shaped the space environment cannot be dismissed. He

identifies the PLA's need to develop a covert space warfare operations as well as the need for the PRC to build a "Space Army." Capabilities of which, Pillsbury specified, include a space-based ASAT network, ship and submarine-launched direct ascent ASAT capabilities, plasma attacks against low-earth orbit (LEO) satellites, and space electronic jamming.[38]

Domestically, current U.S. DoD Space Policy is governed by and nested under the National Space policy of August 2006 and focuses primarily on the operational capabilities enabling our military services to fulfill their respective national security space objectives. Both documents view space as a medium through which military operations can take place--similar to the domains of land, sea, or air. As such, it falls within our national interests to ensure space support, force enhancement, space control, and force application continues unimpeded.[39]

Direct Ascent and Micro-Satellite ASATs

> . . . the offensive capabilities in space should, if necessary, be capable of destroying or temporarily incapacitating all enemy space vehicles that fly in space above our sovereign territory [40]
>
> -- Colonel Li Daguang, PLA 2001

China's interpretation of the "peaceful use of space" (as delineated in the Outer Space treaty of 1967) is clearly inconsistent with their development of the PLA space weapons programs. As early as 2001, rhetoric concerning the development of an offensive "Assassin's Mace" weapon, specifically with space attack capability, began circulating. Colonel Li Daguang makes the particular point that "the offensive capability in space should . . . be capable of destroying . . . all enemy space vehicles that fly in space above our sovereign territory."[41] Later that year the PRC launched the Tsinghua-1, their

first 50 kg micro-satellite, revealing the Kaituozhe-1 (KT-1 Space Launch Vehicle (SLV)) solid-fuel rocket and mobile LEO launch vehicle (Figure 2).

The January 2007 test of a direct-ascent ASAT weapon, for example, in which they confirmed the PLA's ability to destroy satellites operating in a LEO, demonstrated the culmination of years of research and development on their part. The target was an aging Chinese FY-1C weather satellite operating in polar orbit at over 500 miles above the earth. Pentagon officials would later identify the ASAT with the designator "SC-19" and based on the KT-1 SLV. Although this was their third attempt to destroy the same FY-1C satellite, their success confirms they have the capability to compromise the continued operation of many of our LEO ISR platforms used for collection and counterterrorism.[42] Additionally, the debris field formed by said ASAT has the potential to directly compromise the nearly 400 U.S. LEO satellites over the next 20 years.

Figure 2. China's KT series of SLVs. The missile used in the January 2007 Chinese ASAT test is likely to have been a KT-1 (right).
Source: Richard Fisher from the International Assessment and Strategy Center, China's Direct Ascent ASAT, 20 January 2007. http://www.strategycenter.net/research/pubID.142/pub_detail.asp (accessed 18 March 2009).

With respect to this Chinese-created debris field, it is important to note that the two aforementioned U.S. documents, the U.S. DoD Space Policy and the National Space policy of August 2006; both are directly in line with the United Nations Treaties and Principles on Outer Space, 2002. However, as both the U.S. and China are signatories of said treaty, we are both obligated to the "cleanliness" of space under Articles VII and IX. Article VII specifically emphasizes that states are "internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air space or in outer space. . ."[43] Additionally, Article IX covers the responsible use of space in a way that avoids harmful contamination of

outer space; in short, both articles do not ally themselves with the Chinese direct-ascent episode of 2007.

An alternative to a direct-ascent counter-satellite technology are China's co-orbital micro-satellite network and their directed energy endeavors. On micro-satellites there is the BX-1, a 40 kg possible ASAT released on September 27, 2008.[44] Although not conclusively a confirmed ASAT, the BX-1 did make a significantly close pass to the International Space Station at a distance of only 45 km. Thus, the technology exists to release an ultra-small, agile, and lightweight microsatellite to be used as an ASAT platform.

Directed Energy, Kinetic Kill Vehicles, and Space Armies

> Space armies should set up emergency launch units… in order to guarantee that on the day it receives launch orders it will immediately launch space-based fire platforms into orbit.[45]
>
> -- Prof Yuan Selu, PLA NDU 2005

Significantly more sophisticated than either the direct-ascent or co-orbital microsatellites are the directed-energy ASAT. China currently has a policy of using space peacefully and has argued against the militarization of the space environment. However, they have also demonstrated the capabilities that ground-based and airborne high-powered lasers can damage non-hardened thermal controls, optical sensors, and solar power components on LEO satellites. For example, in September 2006, the Pentagon acknowledged that China had fired a high-powered laser at a U.S. reconnaissance satellite flying over Chinese territory.[46]

The PRC recognizes the U.S. utter dependence on space assets and has bolstered their capabilities above and beyond the direct ascent demonstration of 2007. This will

not only potentially enable China to counter our asymmetric space advantage, but also seeks to "guarantee the viability of Chinese nuclear forces in the face of emerging American missile defenses."[47] Research on beam weapon proposals has been detailed by more than 20 authors since 2005. Labeled as "new concept weapons" (or xin gainian wuqi), directed energy weapons cover the gambit of iterations such as high power lasers, microwaves, and particle beam weapons. [48]

Significantly more subtle and clearly reversible technologies are in the completely non-lethal realm such as jammers used to degrade or disrupt functionality without the resultant debris caused by lethal ASAT weapons. Electronic jamming capabilities of the PLA are divided into both hardware interference and command interference. Hardware jamming includes disrupting the electronic surveillance functionality of the U.S. systems. For example, UHF-band satellite communications jammers acquired in the late 90's from the Ukraine give the PLA the indigenous capability to jam common U.S. Army satellite communication bands and GPS receivers. Command jamming, on the other hand, refers to China's jamming of the remote control and remote sensing systems of U.S. military systems. Research and development in intercepting, decoding, and jamming of the ground command is focused on making the satellite deviate from orbit, tumble, exploit, or simply turn off. Command interference is a cost-effective and potentially non-lethal weapon well within the realm of cyberspace.[49]

Targeting satellite terrestrial support infrastructures as well as employing non-contemporary alternatives such as microwaves, particle beams, and electromagnetic pulse weapons, and these future technologies are all just on the PLA's horizon.[50] While the extents of China's ASAT capabilities are uncertain, what is clear is that the PLA is intent

of obtaining a form of Space Superiority. In our extremely heavy reliance on space-based support systems, especially endemic in future and current technologies such as the Future Combat System Brigade Combat Team (FCS (BCT)), Blue Force Tracker, Global Command and Control System, Naval Tactical Data Systems, Unmanned Aerial Systems, and INMARSAT, are all vulnerable targets.

Concerning PLA space operations, the USCC 2008 determined that the PLA "has sufficient capability to meet many of [their] space goals."[51] Through new, space-based assets, they have expanded significantly their electronic and signals intelligence capabilities. This contributes greatly to their military's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) projection capability out to, and including, the southern Pacific Ocean.

Finally, the PLA has been urged to develop space weapons that demonstrate assassin's mace capabilities. As such, they have pushed for covert implementation of space-based fire networks. This would employ standby emergency astronautic launches that would not directly counter international space law. These mobile launch vehicle weapons would employ both space-based directed and kinetic energy capabilities to counter U.S. LEO network systems.[52] Colonel Yuan Zelu, PLA, proposes a total war option that would guarantee that once their space armies receive launch orders, they will immediately fire their weapon systems into orbit.

United States on United States

Domestic Policy on Cyberspace

Under the Comprehensive National Cybersecurity Initiative

Current criminal provisions are essentially reactive by nature as they do not specifically authorize jurisdictional hurdles hampering law enforcement and or military action needed to address cyber-warriors operating abroad. However, both the Federal Information Security Management Act of 2002 (hereafter FIMSA, USC Title 44 §3541, addresses in a later subchapter) along with the Comprehensive National Cybersecurity Initiative (CNCI) take preventative approaches to halting cyber-warriors.

In response to extensive cyber-intrusions into government and DoD computer networks by both known and unknown actors (not necessarily Chinese in origin), the Bush Administration in 2008 established the CNCI as a joint presidential directive. The CNCI establishes the policy, strategy, and guidelines to secure the federal system[53] while collectively seeking to identify both current and emerging cyber-threats, establish protection measures for current and future cyber-vulnerabilities, and delineate responses to address entities wishing to steal or manipulate protected data on secure federal systems. As of this thesis's composition, the U.S. is still within President Obama's 60-day interagency cyber-security review (as of 09 February, 2009). Of note, two major questions have emerged since the Bush Administrations departure that directly relates to this thesis' topic: the adequacy of existing legal authorities for responding to cyber-threats (which will be addressed in follow-on subchapters), and the appropriate roles that both the President and Congress will play in addressing cyber-security.[54]

In addressing the legality of Presidential responses to cyber-threats (up to and including invoking war powers) both the Center for Strategic and International Studies (CSIS) and the Department of Homeland Security (DHS) recommended Executive action to protect U.S. Cyberspace. When addressing the cyber-warriors, our Executive Branch must find support in either the powers granted him as Commander-in-Chief (CINC) under either Article II of the U.S. Constitution, or those congressionally delegated to him via Article I powers.[55] Unfortunately, the CNCI acknowledges that the scope of response and especially the act of invoking war powers in with regards to cyber-warfare defies traditional military strategies and may even fall outside the traditional definitions of war.[56] The CNCI give an example that with regards to private sector domestic cyber-security (e.g. Yahoo! servers) war powers would not likely apply; however, the CINC might well-assert his constitutional oath-based obligation to defend the nation from imminent threats such as foreign cyber-intrusions or cyber-attacks.

In summary, as of this thesis' writing, Congress has yet to authorize the cyber-security reforms proposed by the CNCI. Additionally, the FISMA does not authorize all cyber-security protections, so the CINC is left with one of several options. He can call upon the 2001 Authorization for Use of Military Force if a tie with the 9/11 attackers could be made (doubtful in a case against Chinese cyber-warriors). However, it is more likely that he will follow the advice of Mary Ann Davison, CSO for Oracle, who testified before congress that "given the diversity of potentially hostile entities building cadres of cyberwarrior . . . congress should consider developing a 21st century application of the Monroe Doctrine."[57]

Under U.S. Code

Regardless of the significant cyber-based threats to the U.S. Government and our domestic national interests, the Use of Army and Air Force as Posse Comitatus (PCA, 18 USC §1385) significantly restricts DoD's ability to truly "dominate" Cyberspace. Established as a U.S. Federal Law on June 16, 1878 after the conclusion of the Reconstruction, it expresses that anyone who, "except in cases and under circumstances expressly authorized by the Constitution of Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."[58] Basically, it makes it illegal for the U.S. military to execute the laws of the U.S., specifically in the performance of domestic civilian law enforcement functions.

However, this is not to imply in any way that the U.S. Government is powerless to protect our national interests, especially when the DoD is under attack. 18 USC § 1386 is significantly different from the aforementioned PCA in that it specifically addresses those individuals who attempt to steal, purloin, embezzle, or obtain by false pretense any lock or key to any lock knowing that such lock or key has been adopted by any part of the Department of Defense. Barring future advents of USC specific to Cyberspace, this "key" and its interpretation thereof, can be extended into the virtual realm as those methods and procedures used to ensure DoD authentication, non-repudiation, and encryption of our systems.

10 USC §2224, unlike the PCA, delineates to the Secretary of Defense specific actions such as the establishment of the Defense Information Assurance Program. As such, he is responsible to the National Command Authority for the "continuous

availability, integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Structure."[59] However, these responsibilities are limited by 44 USC §3541 which praises "commercially developed information security products" but recognizes that "the selection of specific technical hardware and software information security solutions should be left to individual agencies. . . ."[60] While this represents the crux of the Federal Information Security Management Act of 2002, it also begs the question, how is the OSD to ensure the integrity of information systems critical to the DoD when agencies can self-determine their software and hardware configurations independently? Additionally, 44 USC §3541 runs contrary to recent testimony given by the director of the Center for Strategic and International Studies, who gave as his top recommendation was a call for regulations and that the private sector "will never deliver adequate security and the government must establish regulatory thresholds for critical infrastructures."[61]

International Policy on Cyberspace--United Nations Charter

> Although there is a considerable body of international law that governs the use of force in Cyberspace, technology does not allow a state to completely prevent computer espionage or computer network attack, nor does it assure that a state can reliably determine the identity of an intruder or attacker in any timely manner.[62]

Jus ad bellum, the law of conflict management or the Latin literal translation of "Justice to War," is a set of rules that govern the resorting to armed conflict and determine whether said conflict is lawful or unlawful in its inception.[63] Contemporary recognition of a state's right to resort to war is captured in Article 2(4) of the Charter of the United Nations. Written in 1945, well before the existence of a Cyberspace, this

article still has basis in today's cyber-conflicts as it redefines for us the principles of jus as bellum. It states that:

> All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in a manner inconsistent with the Purposes of the United Nations.[64]

Unfortunately, the charter neither defines what the threat of force or, more importantly, what constitutes the use of force. Additionally, how does Cyberspace fit into this equation? Assuming that China, or any state for that matter, would never lay claim that neither Computer Network Defense (CND) nor Electronic Protection measures (EP) are an act of aggression; we are left with CNE/ES and CNA/ECM.

With respect to both CNE and ES, we have international precedent from the 1950's through 70's where 22 military intelligence aircrafts were attacked by the former-Soviet Union. In 1960, the Soviet government asserted before a United Nations panel that a specific U-2 flight by the U.S. over Soviet territory constituted an act of aggression. The United Nations disagreed and concluded that while the U-2 flights violated Soviet airspace, the act by itself did not constitute a use of force as dictated by Article 2(4). Interesting point of fact, however, was that due to the political implications of a military aircraft flying over sovereign USSR, military pilots were required to resign their commissions before flying the CIA-owned platform[65]. This case established two presidencies with regards to CNE and ES:

1. All nations are afforded reasonable self-defense response proportionate, if not in kind, to the danger posed by the presence of the trespassing collection assets.
2. If the unlawful, physical penetration of a state's airspace by intelligence aircrafts of another state's is not construed under the U.N. Charter as a use of force, then a

CNE and/or ES taken by one country against another also cannot be construed as a use of force either.

Therefore, so long as the action taken by the victim state is meet principles of proportionality with respect to the danger posed by the presence of the cyber-spy (using ES/CNE methods), the victim state is acting well within the intent of U.S. Article 2(4). Unfortunately, that begs the question, what is a proportionate response?

---

[1]Kristen Gunness, "An Assessment and Analysis of PLA Publication". (FBIS 2005) , X.

[2]Ibid., X-XX.

[3]Zhiqing Han "Combat Worthiness--A New Topic in Non-War Military Actions," (PLA Daily (*Jiefangjun Bao)* 24 July 2008).

[4]Qiao Liang and Wang Xiangsui "Unrestricted Warfare: China's Master Plan to Destroy America". (Pan American Publishing Company 2002) , 122-123.

[5]Ibid., 123.

[6]Ibid., 17-20.

[7]Qingmin Dai "Flexibly Utilization of Battlefield Information Environments, to Gain Advantageous Positions in Combat, through the use of Information Conditions": submitted for inclusion in Peng Chencang's book, "Efforts to Explore Information Warfare Theory Applicable to our Armed Force"s, (Beijing, AMS, 01 Jan 1999), 34-41.

[8]Ibid ., 40.

[9]Ibid., 36.

[10]Ibid.

[11]Timothy L. Thomas *47 China's Electronic Strategies* (Military Review May-June 2001).

[12]Ibid. Gunness, 76

[13]Ibid.; Thomas 47 Strategies

[14]"Interview Transcript: Dai Qingmin, a Delegate of the National People's Congress from the PLA, Talks about Network Security," PLA Daily (*Jiefangjun Bao)*, 14 March 2007.

[15]T'ao Wen *PLA Bent on Seizing Information Control* (translated from Chinese), (Hong Kong Ching Pao 01 Jun 2002).

[16]*Qianwei Bao* (16 Feb 2007) summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

[17]*PLA Daily (Jiefangjun Bao)*, 27 January 2007 summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

[18]Dennis J. Blasko *The Chinese Army Today: Tradition and Transformation for the 21st Century*, (Asian Security Studies, 2006) , 98-107.

[19]*PLA Daily (Jiefangjun Bao)*, 14 June 2007 summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

[20]*Bingqi Zhishi*, December 2006 and *Taipei Times*, 11 March 2007.

[21]Li Chao and Zhou Jinquan *Jamming Effectiveness Evaluation From the Jamming Side* (translated from Chinese), (Chengdu, March and April 2008).

[22]Ibid.

[23]Li Dongxin *Multi-Signal Jamming Technology in Complex Enviroment* (translated from Chinese),(Chengdu, March 2008).

[24]Chen Ximing and Huang Shouyi *DSSS Signal Parameter Estimation* (translated from Chinese), (Chengdu, May 2008).

[25]*Analysts Dismiss "Cyber Spy" Claims*, (China Daily, March 30, 2009) www.china.org.cn accessed 30 March 2009 [no author given].

[26]Interview with Professor Zhu Feng, Professor, School of International Studies, Peking University given on 30 March 2009.

[27]Interview with Qiu Feng, information security expert, given to the Beijing Global Times on 30 March 2009.

[28]Annual Report to Congress: Military Power of the People's Republic of China 2008, Office of the Secretary of Defense; as quoted from the PLA National Defense University book, Joint Space War Campaigns (2005), author Colonel Yuan Zelu.

[29]Annual Report to Congress: Military Power of the People's Republic of China 2008, 17.

[30]Ibid., 20.

[31]Mark Stokes "China's Strategic Modernization: Implications for the United States" (Strategic Studies Institute, 1999), 27.

[32]Ibid Akkad.

[33]Wikipedia, Deloitte Touche Tohmatsu http://en.wikipedia.org/wiki/Deloitte_Touche_Tohmatsu . (accessed 30 March 2009).

[34]Anthony Cordesman and Martin Kleiber "Chinese Military Modernization: Force Development and Strategic Capabilities" (CSIS, 2007).

[35]Annual Report to Congress: Military Power of the People's Republic of China 2008, 3.

[36]Carl Ginter, LCOL, USA: "Space Technology and Network Centric Warfare: A Strategic Paradox" (USAWC, 30 Mar ch 2007).

[37]Richard Fischer, Jr.: "Shenlong Space Plane Advances China's Military Space Potential" (International Assessment and Strategy Center, 17 December 2007).

[38]Ibid Pillsbury.

[39]U.S. Army Command and General Staff College Space Reference Text, March 2008.

[40]Ibid Pillsbury, 10.

[41]Li Daguang, Colonel, PLA, "Space War" (China's National Defense University, 2001).

[42]William J. Broad and David E. Sanger, "Flexing Muscle, China Destroys Satellite in Test" (*New York Times*, 19 January 2007).

[43]United Nations Treaties and Principles on Outer Space, 2002, Article VII.

[44]Richard Fisher: Closer Look: Shenzhou-7's Close Pass by the International Space Station http://www.strategycenter.net/research/pubID.191/pub_detail.asp (accessed 22 May 2009).

[45]Ibid Pillsbury, 11.

[46]Vago Muradian: China Tried to Blind US Sats with Lasers (Defense News, 25 September 2006).

[47] Martin France and Richard Adams. "The Chinese Threat to US Superiority." *High Frontier Journal*, Winter 2005, 18.

[48]Ibid Pillsbury, 14.

[49]Ibid Pillsbury, 26.

[50]Ibid, Annual Report to Congress: Military Power of the People's Republic of China 2008 21.

[51]2008 Report to Congress of the US-China Economic and Security Review Commission (USCC), November, 8.

[52]Ibid Pillsbury, 23-24.

[53]Department of Homeland Security, *Fact Sheet: DHS 2008 End of Year Accomplishments* (18 December 2008).

[54]John Rollins and Anna Henning "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (10 March 2009).

[55]US Constitution Article I, §8 and US Constitution Article II §2 c1.1.

[56]Rollins, 10.

[57]Testimony of Mary Ann Davidson before House Subcommittee on Emerging Threats, Cybersecurity, Science & Technology, 10 May 2009 .

[58]Title 18 US Code §1385, Posse Comitatus Act (1994).

[59]Title 10 US Code §2224, Defense Information Assurance Program (2007).

[60]Title 44 US Code §3541, Information Security.

[61]Testimony of James A. Lewis before House Subcommittee on Emerging Threats, Cybersecurity, Science & Technology, 10 May 2009.

[62]Walter Gary Sharp, Sr.: "Cyberspace and the Use of Force" (Aegis Research Corporation 1999).

[63]Adam Roberts and Richard Guelff: Documents on the Laws of War (Oxford University Press, USA; 3 edition 22 June 2000).

[64]*Charter of the United Nations*, signed 26 June 1945.

[65]*Invention & Technology Magazine*, Volume 22, Number 3.

CHAPTER 3

RESEARCH METHODOLOGY

The methodology to assess these two nations will be to simply collect and analyze the Cyberspace activities and capabilities between the two; then compare each nation side-by-side and line-for-line, but quantitatively based on four criteria as follows:

1. Training: From a strictly academic position, compare and contrast the education and training a PLA cyber-warrior receives as compared to a U.S. Soldier. This will identify training gaps in the U.S. military education system and possible advantages that we have over PLA forces.
2. Weapon systems: Beyond the rudimentary listing of advance computing capabilities or routine hacker scripts, viruses, and DDoS-techniques used in executing typical CNO, what specific cyber-systems do each country posses that can deny, deceive, degrade, or disrupt operations in the cyber-realm with regards to both the means and the mediums through which information is relayed. As this in an unclassified thesis, the U.S. counters will merely list the system name with no description unless common knowledge.
3. Planning: With regards to integration into the planning cycle, how does China's Integrated Network Electronic Warfare (INEW) either differ or expound upon the U.S. Network Centric Warfare.
4. Full Spectrum Operations: From the perspective of the U.S. military, how does the literature review from Chapter 2 map out along the U.S. Army's view of Full Spectrum Operations (FSO)? What precursors to Chinese

PLA activities should we expect through both rhetoric and established precedent?

Analysis of these four should answer my thesis of "to what extent the Chinese cyber-warriors represent a viable threat to both the security and prosperity of our nation as a whole," as well as "ascertain[ing] the U.S. Government's ability to defend and enforce our national interests, both in regards to our own domestic infrastructures as well as our partners abroad from Chinese-directed cyber-attacks"

CHAPTER 4

ANALYSIS

Once again, the purpose of this paper is to determine to what extent the Chinese cyber-warriors represent a viable threat to both the security and prosperity of our nation as a whole. Chapter 4 now takes the lessons from Chapter 2's Literature Review and seeks to introduce an analytical perspective that will evaluate holistically:

1. How the PLA train their cyber warriors from an educational perspective
2. What cyber-weapons the PRC equips their on the battlefield to conduct INEW
3. How the Chinese plan to incorporate their cyber-warriors in major combat operations
4. How do Chinese view the domain of Cyberspace across the entire spectrum of conflict

Training: U.S. vs. PLA Cyber-warrior

The PLA has spent the past several years pursuing a comprehensive build-up from a mass army designed for a protracted war of attrition into one capable of fighting and winning short duration, high-tech wars under "conditions of informatization (sic)."[1] As noted in the 2006 Quadrennial Defense Review, China has the "greatest potential to compete militarily with the U.S. and field disruptive military technologies that could over time offset traditional U.S. military advantages." As mentioned earlier, the PLA's current focus is on preparing for contingencies in the Taiwan Strait, thus supporting their drive for modernization or in their own words informationalization. The scope of this

modernization has increased in recent years, signaled by the high rate of investment in domestic defense supported by scientific and technological innovations.

On the training of these men and women, the responsibilities for offensive and defensive cyber-warfare and their associated education and training are all shared by the PLA, the Ministry of State Security, the Ministry of Communications and the Propaganda Department. In the PLA it appears that cyber-warfare is the primary responsibility of General Staff Department Deputy Director General Chen Xiaogong, who oversees the Third Department of the General Staff Department. As such, it is General Xiaogong's responsibility for executing military cyber-warfare operations that incorporate electronic warfare, and electronic and signals intelligence (ELINT) within not only the PLA, but also the PLAN and PLAAF. The entire Third Department is led General Qui Ruilin, with General Wu Guohua as his technical director. Deputy Directors include General Pan Huizhong, who is also deputy director of the PLA's Central Communication University, General Liu Xiaobei, an encryption specialist, Professor Yang Huida and Professor Liu Meng. Finally, the Fifth Bureau is headed by Professor Yang Jingzong, who is a specialist in communication security as well as information operations.

The training and development of the PLA cyber-warriors is predominantly conducted at the Information Security University in which students are taught in the practice of Information Security (IS) defense and attack techniques, as well as theory in the military arena. Graduation enables the PLA cyber-warriors to work in national defense and all military departments and levels.[2] Of the academic curriculum that is to follow,[3] all is contained within the teaching plan for Military Information Security Studies (MISS) for the PLA. For comparison, the Naval Postgraduate School was

selected, although any post-graduate service school would have produced equivalent results.

U.S. Naval Postgraduate School vs. PLA Military Information Security Studies		
U.S. NPS M.S. in Computer Science	PLA MISS	
(CS2006) An Introduction to Information System Security (4 credits) (CS3600) Information Assurance: Introduction to Computer Security (4 credits) (CS3640) Analysis of DoD Critical Infrastructure Protection (3 credits) (CS3660) Critical Infrastructure Protection (4 credits) (CS3670) Information Assurance: Secure Management of Systems (3 credits) (CS3686) Identity Management Infrastructure (3 credits)	An Introduction to Information Security (1 credit)	Information Security and Information Assurance
(CS2020) Introduction to Programming (4 credits) (CS2071) Fundamental Object-Oriented Programming in C++ (4 credits) (CS2171) C++ as a Second Language (4 credits) (CS3022) Programming Paradigms (4 credits) (CS3071) Advanced Object-Oriented Programming in C++ (4 credits) (CS3113) Introduction to Compiler Writing (3 credits)	Compiler Language (4 credits) C Language Program Design (3 credits) Coding Principles (4 credits) Code Algorithms (2 elective credits) Introduction to Codes (4 credits)	Undergraduate (UG) programming language (in this case, C++)
(CS2073) Fundamental Object-Oriented Programming in Java (4 credits) (CS2170) ADA as a Second Language (4 credits) (CS2173) Java as a Second Language (4 credits) (CS3101) Theory of Formal Languages and Automation (4 credits) (CS3111) Principles of Programming Languages (4 credits)	Not specifically covered in the MISS curriculum as a single course	UG computer programming languages

(CS3502) Computer Communications and Networks (4 credits) (CS3675) Network Vulnerability Assessment (3 credits) (CS3690) Network Security (4 credits)	Network Principles and Communications (6 credits with lab) Computer Fundamentals (2 elective credits)	UG computer and network basics
(CS3060) Database Systems (3 credits)	Data Structures and Algorithms (3 credits) Database Fundamentals and Application (3 credits)	UG Database systems
(CS3610) Information Ethics, Crime, and Law (4 credits)	Information Security Laws and Regulations (1 credit)	UG cyber-law
(CS3030) Operating Systems (3 credits)	Operating Systems (3 credits)	UG OS
(CS4600) Secure Computer Systems (3 credits) (CS4603) Database Security (3 credits) (CS4605) Security Policies, Models, and Formal Methods (3 credits) (CS4614) Advanced Topics in Computer Security (3 credits) (CS4615) Formal Analysis of Cryptographic Protocols (3 credits) (CS4650) Application of Security Evaluation Criteria (3 credits) (CS4678) Advanced Vulnerability Assessment (4 credits)	Network Security Protocols (2 credits) Network Security System Structures (2 credits) Security Evaluation Standards for Information Technology (2 credits) Security Certification Technology and Application (2 credits)	Graduate Level (GL) Network Security
(CS4675) Intrusion Detection and Response (3 credits) (CS4677) Computer Forensics (3 credits)	Network Intrusion Detection and Defending Against Attack (3 credits)	GL Intrusion Detection
Not specifically covered in the NPS curriculum as a single course	Computer Virus Program Design and Application (3 credits) Preventing and Remedying Computer Viruses (2 credits) A Study of Hacker Attack Methods (2 credits) Information Attack and Defense Tactics (2 credits)	GL virus and hack methods

(CS4530) Wireless Mobile Computing (3 credits) (CS4535) Mobile Devices (3 credits) (CS4537) Wireless Data Services (3 credits) (CS4538) Mobile and Wireless Security (3 credits)	Not specifically covered in the MISS curriculum as a single course	GL Wireless
(CS4550) Computer Networks II (4 credits) (CS4552) Network Design and Programming (3 credits) (CS4554) Network Modeling and Analysis (4 credits)	Not specifically covered in the MISS curriculum as a single course	GL Network Design and Modeling

Figure 3. U.S. Naval PG School vs. PLA Military Information Security Studies *Source*: Relevant details pertaining to the PLA MISS extracted via Timothy Thomas' research in "Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy" (Foreign Military Service Office 2007) pg 150; applicable details pertaining to NPS MS in CS via http://www.nps.edu/Admissions/Catalog/index.html in the Naval Postgraduate School Academic Catalog 2009 (accessed 18 March 2009).

It becomes readily apparent that while the PLA do receive advanced specialized training in the areas of virus development and hacking techniques, their curriculum is woefully insufficient when compared to that taught at the U.S. Naval Postgraduate School (NPS) in nearly every category. Granted, the curriculum was laid out in 2002, which explains the PLA's lack of wireless training, however at the time it met the PLA short-term goal of establishing a common, full-time university supporting information security at the undergraduate and professional level.[4] One final note emphasizing the focus of study, PLA's MISS program has 4 required courses on viruses and hacking methods. This compared to the NPS's zero courses begs the question of relevance. It should not be assumed that the PLA is developing better CNA warriors simply because they received a series of virus scripting courses. On the contrary, with little to no

experience in code writing beyond the undergraduate exposure to coding principles, one must question their hacking ability beyond that of a junior script-kiddie.

This in no way implies that the PLA would be ineffective in their application of CNO on the battlefield. However, it does bring forth the question as to both the adaptability and flexibility of the PLA cyberwarrior to the dynamic nature of real-life combat operations against a very capable adversary such as the United States.

Weapons: U.S. vs. PLA Cyber-warrior

As discussed in Chapter 1, the PLA is actively pursuing an assassin's mace weapon that when used will produce devastating results on the U.S. military's ability to continue armed conflict. The application of this weapon system must be decisive in its use of surprise and represents a revolution in military affairs. Listed below are the most popular PLA weapon systems to date separated by the service most-likely to utilize system.

U.S. Army vs PLA	
U.S. Army	People's Liberation Army - Ground[5]
NIPR: Army Knowledge Online (AKO) SIPR: AKO(S)	**All-Army Public Data Exchange Network:** In order provide data exchange services at the national and theatre levels. Responsible for the automatic transmission and exchange of data, image, and text information within the PLA.
Future Combat System (FCS)	**Digitized Army Program:** Inspired by the U.S.A. Future Combat System (FCS) and established in 2001, currently limited to the company and battalion levels; however, includes almost every operational service of the PLA Ground to include Armor, Artillery, the Airborne Corps and Special Operations Forces. **Their specific objective is to identify exploitable weaknesses that can be used by conventional forces (PLA) against a digitized army (U.S.).** Each soldier can transfer real-time image and video battlefield information to C2; each vehicle possesses independent navigation/positioning, battlefield image capturing, target acquisition, audio/image/data transmission, and laser warning and defense.
Advanced Threat IR Countermeasures (ATIRCM) Counter Missile Warning System (CMWS) Chinese system seeks to counter: Bolt-117, JDAM	**Bodyguard Laser-Guided Weapon Countermeasures System:** Loaded in two cross-country trucks and two trailers, the Bodyguard laser countermeasures system comprises five subsystems, including Laser Warning Receivers (LWR), Active Laser Jamming (ALJ), Passive Laser Jamming (PLJ), Central Display Control (CDC) and Power Supply (PS). One system is capable of protecting an area of 6,000~16,000 square meters. The Bodyguard system will be deployed near the target to be protected. When enemy aircraft turns on its laser illuminating to aim the targets, the laser warning receivers deployed around the target will pick up the laser beam and inform the CDC unit. Within seconds the PLJ will launch grenades to form a smoke obstacle over the protected target to block the enemy's laser illuminating. At the same time the ALJ unit will launch similar laser beam to the fake targets some distance away from the protected targets. The fake targets reflects the laser signal back to the enemy's laser guided weapon to misguide it so that it will hit the fake target rather than the real one.
GCCS, JTIDS, NTDS	**Regional Integrated Electronic System ("Qu Dian") - Project 995:** The PLA began to construct a theatre-level command, control, communications, computers, intelligence, surveillance, target-acquisition, reconnaissance (C4ISTAR) network at its southeast coast region in the 1990s. This network, known as Regional Integrated Electronic System (Qu Dian), is an automated battle management system that can support joint operations with combined ground, naval, and air forces.

	The centre of the “Qu Dian” system is a dedicated military communications satellite codenamed FengHuo-1 (FH-1) first launched in January 2000. The Pentagon described that system as "a secure, jam-resistant, high capacity data link communications system for use in a tactical combat." It was China’s first space-based communication platform to provide military units with both C-band and UHF communications. The “Qu Dian” system allows theatre commanders to communicate with and share data with all forces under joint command. The current “Qu Dian” system in southeast China mainly focuses on a possible conflict with Taiwan. The system covers military units within Nanjing and Guangzhou (Fig. 1) military regions. The system includes a theatre joint operation C4I centre (JOC), which is capable of rapidly passing operational orders down the chain of command and moving information to national and theatre level decision makers. The theatre JOC has direct communication links with C4I centers of Nanjing Military Region (MR), Nanjing Military Region Air Force (MRAF), Guangzhou MR, Guangzhou MRAF, Navy Headquarters, East Sea Fleet, maritime task forces and a submarine intelligence centre. The “Qu Dian” system enables theatre commanders to create an integrated battlefield picture, centralizing data from ground, air, naval and space-based platforms for wide dissemination to subordinate units. The system controls a large number of platforms including imagery and radar reconnaissance satellites, airborne early warning and control (AEW&C) aircraft, electronic intelligence (ELINT) aircraft, electronic warfare aircraft, ELINT ships, land-based observation stations, land-based electronic warfare & countermeasure (EW/ELINT) units, etc.
ELINT (1-18Ghz)	**DZ9001 Mobile Electronic Intelligence System:** The DZ9001 is a mobile electronic intelligence (ELINT) system designed to detect, intercept, analyze, identify and record the enemy radar radiation. By collecting and analyzing the signals of enemy radar, their technical parameters and operation modes can be acquired and recorded for both defensive and offensive electronic countermeasures operations such as suppression of air defense (SEAD). The DZ9001 system is composed of 1~8 GHz low-band system, 8~18GHz high-band system and power supply. The high- and low-band systems can operate separately or in together. The system was developed by Jiangnan Electronic & Communications Research Institute (JECOR, also known as 36 Institute) of Jiangxing, Zhejiang Province. The development began in 1984 and the system entered the PLA service in the late 1980s
Prophet System	**JN1105A Communications Jammer:** The JN1105A is a mobile communication countermeasures system designed to locate and jam

	enemy tactical radio communication signals. The system was developed by 36 Institute (now Jiangnan Electronic & Communications Research Institute, JECOR) of Jiangxing, Zhejiang Province in 1982. The JN1105A took part in the 1980s China-Vietnam border conflict and played important roles in the electronic warfare to suppress Vietnamese Army command & control and communications networks. The system can cover the communication frequencies of HF (1.6~30MHz), VHF (30~100MHz), and UHF (100~500MHz). The whole system is carried on a vehicle, but can also be dissembled and carried by several soldiers on specially-designed racks to reach remote areas in mountain and highland
No traditional counter or vulnerable primary system in U.S. arsenal	**JN1601 Communications Jammer:** The JN1601 is an integrated communication countermeasures system designed to search, intercept, monitor, analyze, and jam enemy high-frequency (HF) communication signals. The system can be used as a stand-along system or integrated into other communication countermeasures system. If necessary, the system can also be used for conventional communication purpose. The system is also used for communication and electronic warfare training.
U.S. Navy vs PLA	
U.S. Navy	People's Liberation Army - Navy
Rubicon System	**NRJ5 Ship-Based Electronic Warfare System:** The NRJ5 is a shipborne electronic warfare (EW) suite designed to provide radar and laser warning, as well as to employ electronic/laser countermeasures to neutralize enemy threats. The system provides the capability of surveillance, radar/laser warning, passive and active jamming against various anti-ship weapons. Being modular in design, the NRJ5 system can be easily tailored into different function units to optimize EW capabilities for different classes of naval vessels. The system can be either used as a stand-along EW module, or integrated into the Combat Information Centre (CIC) and other onboard systems to form a complete command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) system.
Chaff	**Seawatch Shipborne Electronic Countermeasures System:** Seawatch is a shipborne electronic and electro-optical countermeasures system designed to provide both passive and active defense against guided weapons (radar-, IR-, TV-, and laser-guidance). The system can be installed on a variety of surface combatant ships from 200 to 4,000 tons. When a hostile laser threat signal is detected by the system's optical sensors, Seawatch gives out warnings, and trigger smoke grenade launchers to generate a smoke screen to protect the carrier ship. If the system receives hostile radar signals through its radar warning

	receivers (RWR), Seawatch system can calculate the best launching parameters for the onboard air-defense or anti-missile weapons, and the best maneuver direction for the carrier ship, based on the threat signal, current sailing data, and meteorological information
Aegis and SPY-1	**HZ100 Shipborne ECM/ELINT System:** The HZ-100 is a shipborne ECM/ELINT system to detect, intercept, analyze and identify the electromagnetic emissions of hostile radar from the sea, shore, and air to acquire information on those radar related weapon systems, providing the carrier ship with the basic intelligence for electronic warfare reactions. The system covers the signal frequency of 2~18 GHz
U.S. Air Force vs PLA	
U.S. Air Force	People's Liberation Army - Air Force
Rivet Joint	**JN1102 Airborne Communications Jamming System:** The JN1102 is an compact airborne communication countermeasure system designed to provide rapid scanning, interception, analysis, monitoring and jamming against hostile ground-to-air C2 communications in the frequency range 20~500MHz. The system is carried by a piston-engine unmanned aerial vehicle (UAV) such as ASN-206. The complete system consists of a UAV-mounted intercept subsystem, a UAV-mounted jamming subsystem and a ground-based intercept and jamming control subsystem.
EA-6B (Navy) EB-52H (cancelled)	**KG300G Airborne Self-Defense Jammer Pod:** The KG300G is an airborne self-defense jammer pod developed by China Electronic Technology Corporation (CETC). The system was designed to be carried by combat aircraft on their external stores stations to perform jamming in I-/J-band against hostile airborne or land-based weapon radar. The pod-contained KG300G is much smaller and more flexible than the internally installed jammer, but with similar performance.

Figure 4. U.S. versus PLA EW and Space weapon systems

As indicated in Figure 4, each U.S. branch has their own respective either equivalent or counter-PLA system in the realm of EW. Although not overtly discussed in historical PLA military exercises along their multiple military regions (Figure 1), one can assume that conducting operations in a complex military environment implies frequency deconfliction to minimize fratricide amongst PLA units.

Planning: U.S. vs. PLA Cyber-warrior

In 2002, Major General Dai Qingmin (discussed in chapters 2-1.b and 2-1.c), the then-Director of the 4th Department of the General Staff Department, published his Wang Dian Yiti Zhan (Introduction to Integrated Network-Electronic Warfare) and his book Direct Information Warfare. With Dai's theories on Battlefield Information Environment (BIE) presented in 1999 as well as Colonels Qiao Liang and Wang Ziangsui's *Unrestricted Warfare*, how does the PLA's plan to implement cyberspace in order to compensate for their military inferiority compete with the U.S. execution of Network Centric Warfare?

Dai presented several interesting arguments in support of Integrated Network-Electronic Warfare (INEW). First, he dissected the two emphasizing that EW's objectives are the disruption of an opponent's acquisition and forwarding of information; while computer network warfare's objectives are to disrupt the opponent's processing and use of information.[6] However, in bringing the two back together, several of Dai's INEW characteristics, while sound in their theoretical application in a combat environment, one finds an equal number of weak arguments as indicated in the following chart:

PLA's Major General Dai Qingmin's characteristics of INEW[7]		
Sound or supported characteristics	**Dai on Battlespace:** Anywhere networks and electromagnetic waves reach can possibly be the site of an information operations attack; thus, INEW will take place in a combat operations space much larger than any current form of combat. **SOUND:** Echoes *Unrestricted Warfare* in its sentiment for breaking through the traditional boundaries of military, trans-military, and non-military warfare; for example, space, economic, and electronic warfare; all of which are viable and well recognized targets of U.S. national power.	**Dai on Effectiveness:** INEW takes as its main targets of attack the normal operation of the information system in the enemy's political, military, economic, and social systems. Therefore, combat effect resulting from INEW is greater than that of any single form of traditional combat operations. **SOUND:** Again, echoes *Unrestricted Warfare*, however, now Dai hits on virtually the same construct used by the U.S. military to define a state's key strengths and weaknesses and describe the operational environment: PMESII, or Political, Military, Economic, Social, Infrastructure, and Information
Unsound or unrealistic practices	**Dai on Combat Methods:** INEW must be coordinated as one in terms of targets for attack and combat opportunities. The integrated plan must reflect in full the basic trend of development and the rules of action. However, also in 2002 Dai stressed the "plebification" trend, emphasizing that the populace can now participate in network warfare far from the front lines.[8] **FLAWED:** Dai is quite unrealistic and somewhat irresponsible in suggesting the public become involved in national affair, and at minimum involved in direct support of military combatants. Even so, his two statements are contradictory without an established means to control Chinese nationalists as he does not provide insight on the handling of rogue citizens.	**Dai on Combat Objectives:** Information systems with their computer networks have become the lifeblood of nations' economies and their armed forces. If these networks become paralyzed, a nation's entire security faces a serious threat. Therefore, as soon as this lifeblood is attacked, the combat power of the armed force will be degraded, or even completely lost. **FLAWED:** INEW's success directly depends on an adversary's complete reliance of their C4ISR in order to conduct <u>any</u> effect military operation. For the U.S. we must be completely dependent on the Global Information Grid and NCW in order for INEW to have the impact he expects. Dai assumes too much as the U.S. has historically dominated the battlespace without the assistance of NCW with the only exception being the most-recent conflict.

Figure 5. Dai Qingmin on Integrated Network-Electronic Warfare (INEW)

The military academic theories of Dai, however, seem to have made the way of other armchair generals focused on fighting the last war, and despite his assertions in support of INEW, his theories are not well demonstrated in current PLA training. Throughout the literature review in support of Chapter 2, the repeated sentiment was that while theory is respected, the PLA trains their forces exactly as they intend to fight. As such, PLA military activities in February 2009 would be a good indicator for how one should expect the Chinese to employ their cyber-warriors in a more-current conflict. For

example, in the Beijing MR (Figure 1), the Special Merit 5th Company has developed a system of training infantry units under complex electromagnetic settings. The 5th Company confronted 9 other companies in rotation; each equipped with significantly stronger, high-tech EA and ISR capabilities. Despite their technological shortcomings, they were ultimately able to work out winning strategies by exploiting their existing transceivers for use in different settings. What is important to note is not the specific technique they used, but rather the fact that the communication units of the PLA ground forces are focusing on proactively testing and improving their combat methods in a variety of realistic confrontations.[9] Not attempting to "capture . . . information supremacy in [both] electromagnetic and network space"[10] as Major General Qingmin would have wanted. In fact, if one assumes that the training methodology used by the PLA is a direct indication of their tactics, techniques, and procedures that will be used in combat, then the Chinese will likely mimic the U.S. network-centric warfare. The literature indicates that the PLA seek to develop a competitive warfighting advantage through the development of well-networked, dispersed forces capable of ensuring continued operations.

Full Spectrum Operations: U.S. vs. PLA Cyber-Warrior

The PLA seek to incorporate both lethal and non-lethal skills if and when they become involved in conflict. Assuming that their training conducted across military regions (Figure 1) over the past 10 years represents the actions that we should expect they would take when exposed to similar operational environment and involved in actual combat what actions would separate their operational themes, and what would their FSOs look like? For Cyberspace, the PLA have demonstrated a very complex and vibrant

spectrum of operations through which they maintain control. As such, figures 3 and 4 both seek to address the PLA's operational themes in a full spectrum operations environment.

In Peacetime Military Engagements the PLA will likely have as its only offensive element more non-discriminatory CNE operations as discussed in 2.2a. Space operations and EW, however, will continue to support ASAT testing (from 2.2c) but only on Chinese space assets and EW jamming within the 7 MRs (Figure 1) and from naval assets. From a defensive standpoint, the PLA will establish and demonstrate the use of EWP in their military exercises while their CND will continue identifying and securing critical PLA assets across the Chinese global information grid (GIG). Finally, for stability operations, the PLA will continue to pursue non-U.S. global positioning-type satellite systems and deter reliance on the U.S.-led system for fear of selected availability.

Operating in the spectrum of Limited Intervention, PLA will enhance their CNE capabilities offensively to include limited CNA as required to test U.S. system defenses for possible future exploitation. In space operations, the PLA will increase employment of directed energy on U.S. IMINT collection platforms.

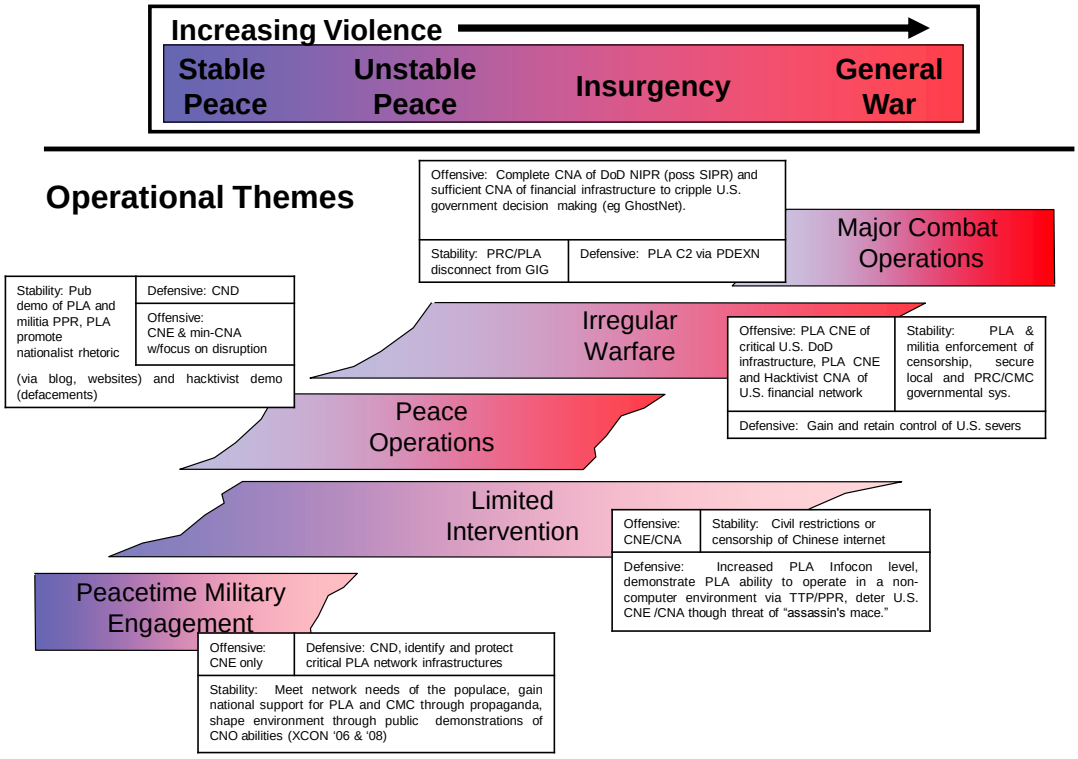

Figure 6. Spectrum of Conflict for PLA cyber-warriors on CNO

[1]Report to Congress, OSD, I.

[2]Timothy Thomas "Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy" (Foreign Military Service Office 2007) , 150.

[3]Ibid ., 152-157.

[4]Ibid., 151.

[5]All PLA Force details derived from www.sinodefence.com a non-government affiliated website run out of the United Kingdom (accessed on 18 October 2008).

[6]Qingmin Dai, Major General, PLA "On Integrating Network Warfare and Electronic Warfare" (Beijing Zhongguo Junshi Kexue 01 February 2002).

[7]Ibid (unless otherwise indicated).

[8]Qingmin Dai Major General, PLA "Direct Information Warfare" (2002) taken from Timothy Thomas "Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy" (Foreign Military Service Office 2007), 124.

[9]Open Source Center Summary, 01-28 February 2009.

[10]Qingmin *On Integrating Network Electronic Warfare.*

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

In an effort to establish an answer to the research statement of determining to what extent the PLA cyber-warriors along with both state and non-state sponsored hackers represent a viable threat to the security and prosperity of our nation as a whole, this chapter will extract the reviews from chapter 2 along with the analysis and conclusions drawn from chapter 4.

In chapter 2, the analysis drew from both Chinese and U.S. literature in an effort to understand the totality of Cyberspace as viewed by both nations. Each country represented their own interpretation with respect to that which the PLA cyber-warriors are capable of accomplishing. From the Chinese perspective, chapter 2 first introduced the difficulties associated with embracing literature generated through the PLA publishing and media systems as they relate to propaganda. However, certain gems, such as *Unrestricted Warfare*, give us unique insight into the PRC and their views on how best to implement cyber-warriors and Chinese nationals. As such, we can conclude that in no uncertain terms, the Chinese fully intend to use completely unconventional methods of warfare that extend beyond exploiting traditional CNO-EW and space assets. Chapter 2 continues by introducing the PLA practices of counter-reconnaissance as well as theories which include integrating a civil-military aspect in CNO (the hacktivists). On EW, research and development beyond traditional communications and satellite jamming parameters is certainly on the PLA's forefront. Finally, Chinese literature responded to the accusations of the GhostNet as anticipated, by pointing back at western nations for

manufacturing the situation. However, it is the depth of GhostNet's penetration into our civil and economic infrastructures that is most worrisome.

The U.S.'s perspective of China follows in Chapter 2 with a strong reminder of the Chinese historical trends of preemptive use of force. Their history, along with rhetoric implying the PLA considering CNO as a first-strike option leaves one to assert that the Chinese are pursuing their asymmetric advantage in CNO. On seizing electromagnetic dominance, the U.S. clearly recognizes the Chinese efforts to emphasize their technological base in C4ISR. Finally, on the significant advances in counter space assets, the January 2007 ASAT is only one of several assassin's mace that the Chinese would like to develop more of.

Unfortunately, legal analysis both into domestic and international cyber-law leave the U.S. military in a dilemma that has yet to be solved. The Comprehensive National Cybersecurity Initiative (CNCI) is still under its 60-day review, and as of this thesis it has yet to identify a clear solution. Guiding principles gleaned from U.S. Code lack the necessary clarification and are contradictory at best. Internationally, we depend upon United Nations Charters generated over 60 years ago which leaves the United States with the vague option of a thus far undefined proportionality against a CNE.

The chapter on Analysis introduces 4 perspectives that were used to evaluate the extent to which Chinese cyber-warriors represent a viable threat to our nation. First, through the assistance of research from the Virtual Dragon, and a cross-comparison with the U.S. Naval Postgraduate School, it became readily apparent that the PLA CNO academic curriculum is woefully insufficient and severely lacks training especially in a variety of necessary computing languages. Unfortunately, as the only PLA Military

Information Security Studies curriculum was from 2002, at this time, there is no way to confirm that the coursework has not expanded to either mimic U.S. training, or build to a level beyond our own.

The second perspective seeks to analyze both the equipment capabilities and our equivalent systems. This list is limited in its applicability as there is neither a listing to indicate the number of actual systems in the PLA inventory, nor the relative experience in each system. Throughout the literature review there are references to actual military exercises incorporating the PLA operating in a complex electro-magnetic environment. However, rarely will periodicals such as *PLA Daily* list the specific system by name. One critical gem from all this: first the PLA has implemented an FCS-type program with the sole objective of identifying exploitable weaknesses in U.S. systems. As such, we can expect future combat to be extremely FCS-unfriendly.

The third analysis sought to extract the PLA planning and implementation procedures for the Chinese cyber-warriors. To do this, Major General Dai Qingmin's works were dissected starting from his Battlefield Information Environment in 1999 to an interview several years later. Two critical holes in his theory are discussed implying that his INEW theories will remain exactly that: a theory. Chinese military exercises from 2000 till February 2009 only discuss informationalization along with the modernization of their force. Terms implying a counter-Network Centric Warfare model such as INEW are reserved for academia.

Finally, the fourth analysis takes the highpoints from the thesis to generate a Full Spectrum Operations (FSO) graphic depicting likely PLA actions along the spectrum of

conflict. The main focus of which is the CNO capabilities but space and EW are viable options as well.

In conclusion, in determining to what extent the PLA cyber-warriors represent a viable threat to the security and prosperity of our nation, the answer most certainly is "yes." With that in mind one must surmise from this thesis that the threat is currently limited in nature, but highly demonstrative in potential. For example--despite the fact that the PLA cyber-warriors are at best script-kiddies when it comes to CNO, immature and non-expeditionary when it comes to EW, and neutralized of their asymmetric advantage by our 2008 ASAT demonstration--they have demonstrated exponential growth and development since the publishing of *Unrestricted Warfare* in their MR exercises. Their theories and application of military theory mimics our own to a great extent, however a coordinated INEW assault is unlikely considering their lack of CNO training.

Recommendations for future research are as follows:

1. Further research on the PLA EW systems above the unclassified level. For example, specifically how do the jamming capabilities of the PLA systems compare with the U.S. military's?
2. Current training pipeline and operational employment of the PLA CNO units throughout the MR. For example, are the PLA cyber-warriors simply system administrators or capable combat multipliers?
3. What is the Chinese legal precedent on cyberspace defining their use of force? Additionally, what is the specific legal protocol China uses in

dealing with hacktivists? Is there a clearly defined C2 structure through which the PRC is able to task Chinese nationals? What are the exploitable vulnerabilities in said structure?

GLOSSARY

Assassin's Mace. China's future "shock and awe;" devastating enough to deter any further U.S. military action in a crisis; the application of a weapon system that is decisive in its use of surprise and represents a revolution in military affairs (RMA)

Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)

Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks (JP 3-13)

Computer Network Defense (CND). Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks (JP 3-13)

CNO. Computer Network Operations. CNA, CNE & CND

Cyberspace. JP 1-02 of October 2008 defines it as: A global domain within the information environment consisting of the: interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The Quadrennial Roles and Missions Review Report 2009 specify the domain as "decentralized" where "power can be wielded remotely, instantaneously, inexpensively, and anonymously." However, for the purposes of this thesis, *Cyberspace* will include not only the hardware upon which information is stored, but also the medium upon which this information travels, to include space.

Cyber-Warriors. Not defined through Joint Publication or other recognized military publication, however, for the purposes of this thesis, a cyber-warrior is a state-sponsored soldier or civilian who is either backed financially or through equipping and training and is able to "effectively" operate and fight in cyberspace.

DDoS. Distributed Denial of Service. Is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DDoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the

communication media between the intended users and the victim so that they can no longer communicate adequately.

Electronic Attack (EA). Division of electronic warfare involving the use of electromagnetic energy, directed energy or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-13.1)

Electronic Counter Measures (ECM). A subsection of EW which includes any sort of electrical or electronic device designed to trick of deceive enemy radar, sonar, or other detection systems (e.g. IR and Laser). (JP 3-13)

Electronic Protection (EP). That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 3-13)

Electronic Warfare Support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 3-13)

Electronic Warfare (EW). Refers to any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary. EW includes three major subdivisions: EA, electronic protection (EP), and electronic warfare support (ES). (JP 3-13)

Information Operations (IO). The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

INEW Integrated Network Electronic Warfare. According to Dai Qingmin, refers to a series of combat operations that use the integration of electronic warfare and computer network warfare measures to disrupt the normal operation of enemy battlefield information systems while protecting one's own, with the objective of seizing information superiority--similar to the U.S. definition of IO.

People’s Liberation Army (PLA). For the purposes of this thesis, the term 'People's Liberation Army' implies the land, naval, and air military services (unless otherwise specified, for example: PLAN or PLAAF). This includes the police, and the intelligence services of the Communist Government of the People's Republic of China, and any member of any such service or of such police

APPENDIX

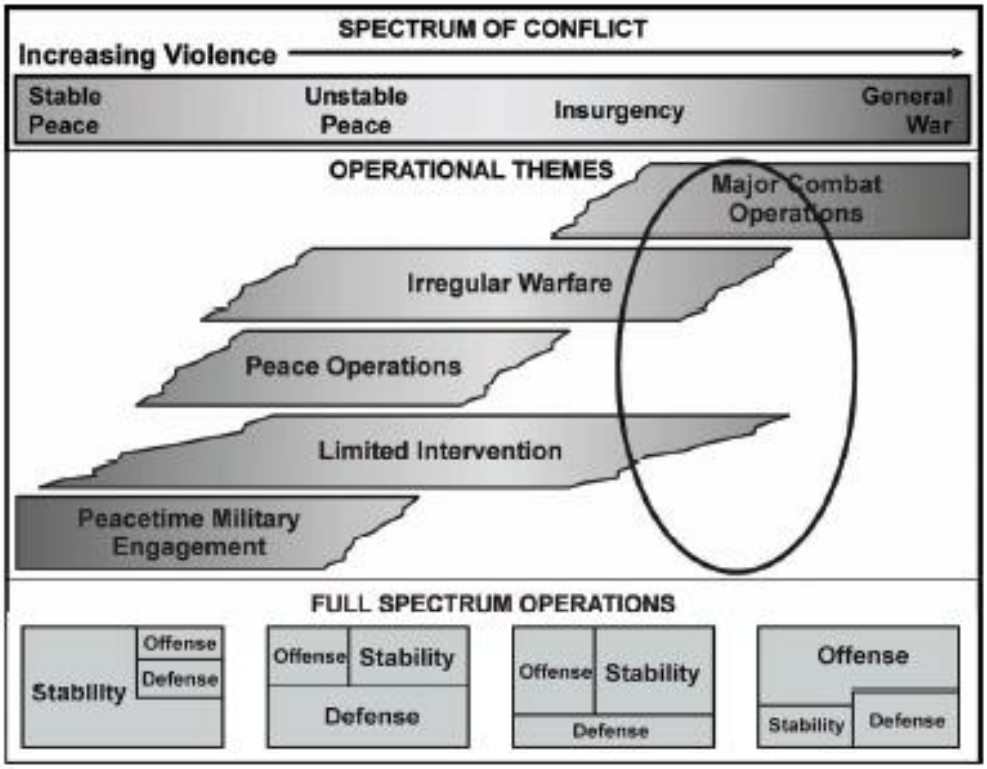

Figure 1 Spectrum of Conflict from U.S. Army Field Manual 7-0.

Field Manual (FM) 7-0, *Training for Full Spectrum Operations*, establishes the Army's keystone doctrine for training. It addresses the fundamentals of training modular, expeditionary Army forces to conduct full spectrum operations (FSO)--simultaneous offensive, defensive, and stability or civil support operations--in an era of persistent conflict.

-Paraphrased from FM 7-0, page iii, 12 December 2008

BIBLIOGRAPHY

United States Sources

2007 Report to Congress of the US-China Economic and Security Review Commission (USCC), November 2007, 96. http://www.uscc.gov/annual_report/2007/report_to_congress.pdf (accessed 22 May 2009).

2008 Report to Congress of the US-China Economic and Security Review Commission (USCC), November.

Annual Report to Congress: Military Power of the People's Republic of China 2008, Office of the Secretary of Defense.

Annual Report to Congress: Military Power of the People's Republic of China 2008, Office of the Secretary of Defense; as quoted from the PLA National Defense University book, Joint Space War Campaigns (2005), author Colonel Yuan Zelu.

Blasko, Dennis J. *The Chinese Army Today: Tradition and Transformation for the 21st Century*, (Asian Security Studies, 2006).

Brenner, Bill: Search Security, *How the China Syndrome Doomed 3M Merger Deal*, 21. February 2008 http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1301833,00.html (accessed 18 October 2008).

Bridis, Ted: USA Today, *State Department Got Mai – and Hackers* http://www.usatoday.com/tech/products/2007-04-18-2250474372_x.*htm* (accessed 22 May 2009).

Broad, William J. and Sanger, David E.: "Flexing Muscle, China Destroys Satellite in Test" (*New York Times*, 19 January 2007).

Bush, Richard C. and Michael E. O'Hanlon, "A War Like No Other: The Truth About China's Challenge to America" (John Wiley & Sons, Inc. 2007).

Charter of the United Nations, signed 26 June 1945.

Cordesman, Anthony and Kleiber, Martin: "Chinese Military Modernization: Force Development and Strategic Capabilities" (CSIS, 2007).

Cyber Attacks During the War on Terrorism: A Predictive Analysis, (Institute for Security Technology Studies at Dartmouth College, 22 Sepember 2001).

Department of Homeland Security, *Fact Sheet: DHS 2008 End of Year Accomplishments* (18 December 2008).

Elegant, Simon: *Enemies at the Firewall*. http://www.time.com/time/magazine/article/0,9171,1692063,00.html (accessed 25 January 2009).

Fahrenkrug, David T. LCOL, USAF: Air University http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html (accessed 18 October 2008).

Fischer, Richard Jr.: "Shenlong Space Plane Advances China's Military Space Potential" (International Assessment and Strategy Center, 17 December 2007).

Fisher, Richard: Closer Look: Shenzhou-7's Close Pass by the International Space Station http://www.strategycenter.net/research/pubID.191/pub_detail.asp (accessed 22 May 2009).

Gaudin, Sharon "China to Use Computer Viruses as Cyberwarfare Strike First," *Newspaper*, 29 May 2007.

Ginter, Carl (LCOL, USA): "Space Technology and Network Centric Warfare: A Strategic Paradox" (USAWC, 30 March 2007).

Gunness, Kristen "An Assessment and Analysis of PLA Publication" (FBIS 2005).

Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers Invention & Technology Magazine*, 22, no. 3.

Kestenbaum, David: *National Public Radio, Chinese Missile Destroys satellite in 500-mile Orbit* http://www.npr.org/templates/story/story.php?storyId=6923805 (accessed 22 May 2009).

Liu, Melinda: *High-Tech Hunger Newsweek* from magazine dated Jan 16, 2006 http://www.newsweek.com/id/47443/page/3 (accessed 22 May 2009).

Muradian, Vago: China Tried to Blind US Sats with Lasers (Defense News, 25 September 2006).

Onley, Dawn S. and Wait, Patience: Government Computer News, *Red Strom Rising* http://www.gcn.com/print/25_25/41716-1.html?page=2 (accessed 18 October 2008).

Open Source Center Summary, 01-28 February 2009.

Pillsbury, Michael P. "An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines," (Report to the U.S.-China Economic and Security Review Commission, 19 January 2007).

Roberts, Adam and Guelff, Richard: Documents on the Laws of War (Oxford University Press, USA; 3 edition 22 June 2000).

Rollins, John and Henning, Anna: "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (10 March 2009).

Schriner, David given before the Joint Economic Committee, United States Congress, on 25 February 1998 http://www.freedomdomain.com/weathercontrol/ jointhearing.html (accessed 22 May 2009).

Sharp, Walter Gary Sr. *Cyberspace and the Use of Force*, (Aegis Research Corporation 1999).

Stokes, Mark: "China's Strategic Modernization: Implications for the United States" (Strategic Studies Institute, 1999).

Testimony of James A. Lewis before House Subcommittee on Emerging Threats, Cybersecurity, Science & Technology, 10 May 2009.

Testimony of Mary Ann Davidson before House Subcommittee on Emerging Threats, Cybersecurity, Science & Technology, 10 May 2009.

The National Strategy for Maritime Security, 20 September 2005 http://www.whitehouse.gov/homeland/maritime-security.html (accessed 18 October 2008).

Thomas, Timothy "Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy" (Foreign Military Service Office 2007).

Timothy L. Thomas "47 China's Electronic Strategies." *Military Review* (May-June 2001).

Title 10 US Code §2224, Defense Information Assurance Program (2007).

Title 18 US Code §1385, Posse Comitatus Act (1994).

Title 44 US Code §3541, Information Security.

U.S. Army Command and General Staff College Space Reference Text, March 2008.

United Nations Treaties and Principles on Outer Space, 2002.

US Constitution Article I, §8 and US Constitution Article II §2 c1.1.

Vellucci, Frederic and Ferguson, Collins and et al, *The Science of PLA Training: Analysis and Overview of PLA Training Theory* (Center for Naval Analysis, China Studies, February 2009).

Chinese Sources

"Interview Transcript: Dai Qingmin, a Delegate of the National People's Congress from the PLA, Talks about Network Security," *PLA Daily* (*Jiefangjun Bao),* 14 March 2007.

Analysts Dismiss "Cyber Spy" Claims, (China Daily, March 30, 2009) www.china.org.cn accessed 30 March 2009 [no author given].

Chao, Li and Jinquan, Zhou: *Jamming Effectiveness Evaluation From the Jamming Side* (translated from Chinese), (Chengdu, March and April 2008).

China's National Defense in 2006, Chapter 2, http://www.china.org.cn/english/features/book/194421.htm (accessed 22 May 2009).

Daguang, Li (Colonel, PLA), "Space War" (China's National Defense University, 2001).

Dai, Qingmin (Major General, PLA): "Direct Information Warfare" (2002) taken from Timothy Thomas "Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy" (Foreign Military Service Office 2007), 124.

Dai, Qingmin (Major General, PLA): "On Integrating Network Warfare and Electronic Warfare" (Beijing Zhongguo Junshi Kexue 01 February 2002).

Dai, Qingmin "Flexibly Utilization of Battlefield Information Environments, to Gain Advantageous Positions in Combat, through the use of Information Conditions": submitted for inclusion in Peng Chencang's book, "Efforts to Explore Information Warfare Theory Applicable to our Armed Force"s, (Beijing, AMS, 1 January 1999).

Dongxin, Li: *Multi-Signal Jamming Technology in Complex Enviroment* (translated from Chinese),(Chengdu, March 2008).

Han, Zhiqing "Combat Worthiness—A New Topic in Non-War Military Actions," (*PLA Daily* (*Jiefangjun Bao)* 24 July 2008).

Interview with Professor Zhu Feng, Professor, School of International Studies, Peking University given on 30 March 2009.

Interview with Qiu Feng, information security expert, given to the Beijing Global Times on 30 March 2009.

Liang, Qiao and Xiangsui, Wang *Unrestricted Warfare: China's Master Plan to Destroy America*. (Pan American Publishing Company 2002).

PLA Daily (Jiefangjun Bao), 14 June 2007 summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

PLA Daily (Jiefangjun Bao), 27 January 2007 summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

PRC Taiwan Affairs Office and the Information Office of the State Council (2005)

Qianwei Bao (16 Feb 2007) summarized in *China: PLA Training Emphasizes Countermeasures Against Imagery Reconnaissance* (Open Source Center, 31 July 2007).

US Spyplane Crashing Chinese Jet: Pro-China Hackers Invade US Government Website. http://www.china.org.cn/english/12150.htm (accessed 22 May 2009).

Wen, T'ao: *PLA Bent on Seizing Information Control* (translated from Chinese), (Hong Kong Ching Pao 1 Jun 2002).

Ximing, Chen and Shouyi, Huang: *DSSS Signal Parameter Estimation* (translated from Chinese), (Chengdu, May 2008).

Additional Sources

Akkad, Omar El: *Canadian Researcher in Toronto Uncovers Worldwide 'Cyber-Spy Network'* (The Globe and Mail, Toronto) 30 March 2009.

All PLA Force details derived from www.sinodefence.com a non-government affiliated website run out of the United Kingdom.

Bingqi Zhishi, December 2006 and *Taipei Times*, 11 March 2007.

Downloaded from the Indonesian website www.kobudi.co.id on 24 October 2005 and posted on www.juntuan.cn/user1/2344/archives/2005/9612.shtml (accessed on 22 October 2008).

Wikipedia, Deloitte Touche Tohmatsu http://en.wikipedia.org/wiki/ Deloitte_Touche_Tohmatsu (accessed on 30 March 2009).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

COL Wayne A. Parks
Director, U.S. Army Computer Network Operations and Electronic Warfare Proponent
950 Bluntville Ave
Fort Leavenworth, KS 66027-2301

Mr. Bob A. King
Department of Joint, Interagency and Multinational Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Dr. Plaudy M. Meadows III
Senior Program Manager, National Security Solutions
Science Applications International Corporations (SAIC)
1145 N. Second Street
Leavenworth, KS 66048

Timothy L, Thomas, M.A.
Foreign Military Studies Office (FMSO)
604 Lowe Drive
Fort Leavenworth, KS 66027-2301